Oman Chapter of Arabian Journal of Business and Management Review 10(4), 2021, 99-103
An Open Access Journal
ISSN: 2617-3190

Arabian Journal of Business and Management Review (Oman Chapter)

Research Article | Homepage: www.arabianjbmr.com | AGJ

UTILIZATION OF STRATEGIES FOR ENSURING EFFECTIVE SECURITY OF DATA IN GOVERNMENT PARASTATALS IN ABIA STATE

Dr. Faith Chukwudi Nwaukwa
Libral IT Resource/Consult Ltd. Akure, Ondo State, Nigeria. Corresponding Email: faithnwaukwa1136@gmail.com
Peggy Onyefuruchi Anioke
Department of Office Technology and Management Department, Federal Polytechnic, Damaturu.
Email: faithnwaukwa1136@gmail.com

ARTICLE INFO

Keywords:
Strategies, Data Security, Government Parastatal Network Control Strategy.

Received: Oct 09, 2021
Accepted: Nov 15, 2021
Published: Dec 05, 2021

ABSTRACT

The need to protect data of government parastatals from unauthorized access and breaches necessitated this study. The study ascertained the utilization of strategies for ensuring the security of data in government parastatals in Abia State. One research question and one null hypothesis guided the study. The study adopted survey research design, with a population of 351 data managers in government parastatals studied without sampling. A-14 item structured questionnaire was used to collect data for the study. The face and content validity of the instrument was determined using four experts while the reliability was established using pilot-test and data obtained calculated using Cronbach Alpha formula which yielded correlation coefficient of .87. Descriptive mean and standard deviation were used to answer the research question while ANOVA was used to test the null hypothesis at .05 significant level. Findings revealed that office employees in government parastatals in Abia State utilize network control strategy to a low extent in ensuring security of data. Years of working experience of data managers did not significantly influence their mean responses in this regard. Hence, the researchers concluded that more training/re-training of office staff is needed on how to utilize network control strategy to ensure effective security of data in government parastatals in Abia State. It was recommended among others that; management of government parastatals in Abia State should organize regular data security training workshops for all their office staff to enable them up-data their skills and competencies in utilizing network control strategy for security of organizations' data.

1. INTRODUCTION

Today, many organizations are gathering and sharing an exponentially increasing amount of private and frequently sensitive data, partly as a result of technology advancements, lower data storage costs, the growth of the internet, and the appearance of significant data brokerage firms. However, the dangers any organization confronts from data loss and security breaches have increased along with the amount of data it generates and collects. In fact, numerous business organizations throughout the world have had data breaches that resulted in data loss or destruction, legal liability, a decline in customer trust, or monetary losses. Defects in data security and privacy can have a lasting negative impact on an organization's finance, not to mention its reputation, credibility, and relationships with its customers. Organizations (especially public organizations) must make sure that all data are safeguarded from unauthorized users in order to ensure operational efficiency and consistently meet the demands of the teeming public. Data are an organization's most valuable asset, and it is the duty of every organization to make sure that they are accurately, promptly, and adequately secured. Data are items of information created and saved electronically or manually in files (a computer system). Individuals and organizations rely on data held by organizations as assets to help the m make wise decisions (Thompson, Hertzberg & Sullivan, 2011). Data may be retained by an organization as a custodian of that data or may belong to the organization itself. Data are assets gathered by organizations to assist and improve decision-making and achieve organizational goals, according to Shomrani, Fathy and Jambi (2017). On the other side, data security entails safeguarding information, such as databases, from corrosive agents and the unintended acts of unauthorized users. It basically refers to safeguarding data theft, damage, and undesirable behaviour by unauthorized users. According to Lynch (2022), it is the process of securing company data and avoiding its loss due to illegal access. This involves defending ones or organization's data from attacks that can damage or modify it, as well as attacks that can encrypt or destroy it like ransomware.

On the other hand, a strategy is a plan that is meant to accomplish a specific goals or a method of carrying out a plan deftly (Hornby, 2018). Strategies are seen as defenses against enemy attacks, in this case, other hackers and data thefts, or on opportunities to take advantage of within the corporation to obtain an advantage over others (Kitonga, Bichanga & Muema, 2016). In this study, strategies are plans and processes outlined by management of government parastatals to properly secure their data from loss, damage, or theft. In Nigerian tertiary institutions, data security is covered as part of the data management course in the business education programme. Business education is a skill-based programme that prepares students for independent living or meaningful work. It is an aspect of vocation education programme that instills in its participants the attitudes, knowledge, skills, and competencies necessary for obtaining meaningful employment in contemporary workplace (Sani, Mohammed & Aliyu, 2017). The management, communication, database management, ethical and human relations, scientific, and 21st century technical necessities for administrative/clerical fieldworks and self-reliance are all emphasized in the

business education curriculum (FRN, 2013). The course provides a range of abilities in management, office technology and management (OTM), marketing, and accounting. A graduate of a business education programme is therefore expected to have gained the necessary data security management skills to be able to securely manage sensitive organizational and personal data. Ifejika (2015) pointed out that business education gives students the knowledge and abilities to gather, evaluate, safeguard, and properly dispose of data.

Government parastatals encompass a broad range of economic entities, including statutory corporations and commercial enterprises founded and partially or entirely owned by the government in the public interest. The range of services they offer is typically wide enough to justify their creation as independent organizations separate from regular government department activities. In addition to providing significant freedom compared to the rigorous requirements of the public service, the laws establishing them also provide some degree of autonomy. Government parastatals support socio-economic development by offering the country a wide range of goods and services necessary for humanity, including among others, water, energy, food, and health. Clearly, data are essential to the existence of many government parastatals. To safeguard their data against breaches and compromise, several government parastatals around the world have made data security measures a top priority. Government parastatals in industrialized nations understand the importance of data security in ensuring that each user has the appropriate access to data, and that no sensitive data is overexposed. Al-Awadi and Renaud (2016) argued that in light of this, data security should necessitate a thorough and integrated approach encompassing both management and workers of government parastatals. Data can generally be protected in government parastatals using a wide range of strategies. The Cloud Security Alliance (2012) listed data security techniques, data security auditing, and real-time data security/compliance monitoring as strategies for protecting data in organizations. Shah, Ahmed and Soomro (2016) proposed various technology strategy such as (anti-virus, encryption technology, firewall security, data security, login ID and password, keystroke dynamics and platform security). However, this study focused on how to effectively secure data in government parastatals by using network control mechanisms.

Network control strategy involves setting up firewalls, perimeter alarms, automatic login, encryption (storage and transmission), user verification, password management, and access controls (Ponemon Institute, 2010). As part of this strategy, strong lock codes and password must also be set up, users must be prevented from installing unapproved programmes, full disk encryption must be enforced to secure data on devices, and remote data wipes ad device tracking are permitted. Ray (2013) suggested using biometrics (matching fingerprint, iris pattern, or facial features) and built-in-two factor authentication as powerful authentication and authorization procedures in addition to user name and password, security questions, PIN numbers, and biometrics. Others include a mobile device, an e-mail account, and ID car, or a security token (such as smart cards, key fobs, and USB keys). In the case of a mobile device, ownership can be verified by sending a one-time code to a device that has been pre-registered with the organization) (Privacy Technical Assistance Center (PTAC), 2015). While it is true that some data may be lost or destroyed due to negligence, an accident, or even malicious attacks, it is far simpler to erase or change data that is contained in electronic files and permanently lose the data. The loss of crucial data could be terrible in government parastatals, but it can typically be recreated at home or in school. This is due to the possibility of damaging the government's privacy by exposing sensitive information to the broader public. Additionally, it can make it more challenging for managers and directors of government parastatals to locate the data they need to develop, put into practice, and evaluate policies, as well as to oversee crucial human and financial resources. This condition can make it more difficult to implement administrative and economic reform programmes that aim to increase efficiency, accountability, and citizen services. Furthermore, the loss of data may make it very impossible to assign blame for actions and hold employees responsible.

This study sought the opinions of data managers in government parastatals in Abia State. In this role, data managers who are seen as senior employees or higher-level officers oversee, supervise, and manage the work tasks of subordinate employees to meet organizational objectives. They supervise, foster, and support friendly working relationships among junior workers as professional employees. They may therefore more easily determine whether at government parastatals, employees are using network control strategy to secure data effectively within their organization. Data managers, who can be either male or female, are expected to have both technical and non-technical capabilities, administrative and leadership abilities, as well as the managerial abilities needed to coordinate the organization, execute, and oversight of employees' data handling. Employees should occasionally adjust their focus in order to face these issues because technological advancements are dynamic and bring with them problems with data security in organizations. Employees will therefore look for the necessary strategies to safeguard the data of their organizations against loss, damage, or theft. However, problems with financial scandals, corruption, purposeful data destruction following financial misappropriation to cover up such cases, persistent data loss by management and employees, and hacking of crucial information (data) of both the federal and state parastatals suggest that the strategy under investigation is not being used for data security very much. Data theft, destruction, and loss are significant corporate management difficulties that government parastatals in Nigeria face, according to the researchers' cursory observations. These have reduced the operational effectiveness and eroded public confidence in their operations.

Depending on the data managers' level of experience, different network control strategies may be used for successful data protection. Because, they have more opportunities than less experienced managers to attend training and retraining programmes, workshops, data security summits, and other data security management programmes both inside and outside the country, experienced data managers may rate the strategy's utilization as utilized. When compared to managers with less expertise, Chen (2013) asserted that experienced data managers have throughout the years established effective ways for securing the data of their firm. The necessity for this study is made more urgent by alarming pace at which data are lost, corrupted, hacked, and damaged in government parastatals throughout Nigeria, notably Abia State.

1.1 Statement of the Problem

The unsatisfactory manner in which data in government parastatals are hacked, damaged, lost and destroyed on daily basis due to human error, hardware failure, software corruption, computer viruses, data theft and natural disaster among others has become a cause for worry for the tax payers whose money are used to establish these parastatals. Data insecurity exposes critical corporate information to the general public thereby eroding the organization's privacy, and making it ever more difficult for managers/directors of public organizations to retrieve information needed to formulate, implement, and monitor policies and to manage key personnel and financial resources. As a result, employees of government parastatals must utilize laid down effective strategies to ensure that their data are protected.

Although, there are numerous strategies abound for effective security of data, however, as indicated by the daily complaints of data theft, loss, and destruction that continue to negatively impact the efficient operations of public organizations, it appears that the majority of the strategies for effective security of data are not known to and implemented by employees of government parastatals. The issue with this study is that it is unclear to what extent employees of government parastatals in Abia State are using strategies to ensure good data security. The pursuit of this information is crucial because it will enable government parastatals to manage data security effectively. Hence, the study specifically determined the extent of (1) utilization of network control strategy for ensuring effective security of data in government parastatals in Abia State.

1.2 Research Questions

The following research questions guided the study;

(1) To what extent is network control strategy utilized for ensuring effective security of data in government parastatals in Abia State?

1.3 Research Hypotheses

The following null hypotheses were tested at 0.05 level of significance;

There is no significant difference in the mean ratings of data managers on the extent of utilization of network control strategy for ensuring effective security of data in government parastatals in Abia State based on years of working experience (11 years and above/6 – 10 years/1-5 years).

2. METHODS

The design adopted survey researcher design. It was carried out in Abia State. The population of 351 data managers working in government parastatals in Abia State (Source: Office of the Head of Services in Abia States as at April 13th 2021) was studied without sampling. Structured questionnaire titled "Utilization of Strategies for Ensuring Effective Security of Data in Government Parastatals Questionnaire (USEESD-GPQ)" was used for data collection. The questionnaire consisted of two sections A and B. Section A contained item on demographic information of the respondents such as years of working experience while Section B contained 14 items in respect to the research question, structured on five point rating scale of Very Great Extent (VGE), Great Extent (GE), Moderately Extent (ME), Low Extent (LE) and Very Low Extent (VLE). The face and content validity of the instrument was established using the opinions of four experts; two experts in Data Security Management, one expert from Business Education, and one expert from Measurement and Evaluation. The reliability of the instrument was established using pilot-test and data were calculated using Cronbach Alpha formula which yielded correlation coefficient of .87. The researcher administered 351 copies of questionnaire to the respondents with the help of three research assistants while 342 copies were returned and found usable. Data collected were analyzed using mean and standard deviation to answer the research question and determine the homogeneity of the respondents' opinions. Analysis of Variance (ANOVA) was used to test the null hypothesis at .05 level of significance. A hypothesis was rejected where the p-value is less than the alpha value but accepted where the p-value is greater or equal to the alpha value. All the analyses were done using SPSS version 23.

3. RESULTS

Research Question 1: To what extent is network control strategy utilized for ensuring effective security of data in government parastatals in Abia State?

Table 1

Respondents' mean ratings and standard deviation on the extent network control strategy is utilized for ensuring effective security of data (n = 342)

S/N	Items on Utilization of Network Control Strategy	$\bar{X}$	SD	Remarks
1	Employees ensure that their office computers have up-to-date anti-virus to protect data from virus attacks	3.45	.87	Moderate Extent
2	Employees use passwords to ensure unauthorized installation of malicious applications on the office computers	2.56	.51	Moderate Extent
3	Employees use cover screen-lock to prevent unauthorized access to data stored in office computers	3.21	.66	Moderate Extent
4	Employees set up firewalls on their office computers to protect data from hackers	1.65	.81	Low Extent
5	Employees use built-in two-factor authentication to protect sensitive organizations' data from breach	1.49	.76	Very Low Extent
6	Employees abstain from unauthorized installation of applications in the office system	1.57	.61	Low Extent
7	Employees ensure that they do not upon e-mail messages without first scanning them so as to prevent virus attacks	1.41	.91	Very Low Extent
8	Employees use matching fingerprint to protect data stored in the office computers from unauthorized access	1.39	.82	Very Low Extent
9	Employees ensure that they do not use office computers to download applications over the internet	2.39	.66	Low Extent
10	Employees use security token such as smart cards, and USB keys to prevent authorized access to data stored in the office computers	1.57	.67	Low Extent
11	Employees connect only scanned and certified virus free USB drives to office computers	1.89	.52	Low Extent
12	Employees connect their office computers to internet through only a secure wireless network	1.50	.61	Low Extent
13	Employees report all lost/stolen devices to organization's IT officers immediately	3.44	.81	Moderate Extent

14	Employees report all data loss or breach immediately to IT officers	2.58	.54	Moderate Extent
	Cluster Mean	1.88		Low Extent

The analysis of data in Table 1 show that network control strategy is utilized to a low extent by employees for ensuring effective security of data in government parastatals in Abia State. This is shown by the cluster mean of 1.88 which fell within the low extent category. The item by item analysis indicates that out of 14 items listed utilization of network control strategy, items 1, 2, 3, 13 and 14 are utilized to a moderate extent with mean ranging from 2.56 to 3.45, items 4, 6, 9, 10, 11 and 12 are utilized to a low extent with mean ranging from 1.50 to 2.39 while the remaining 3 items are utilized to a very low extent with mean ranging from 1.39 to 1.49. The standard deviation for all the items is within the same range meaning that the respondents are not wide apart in their mean ratings.

Hypothesis 1: There is no significant difference in the mean ratings of data managers of government parastatals in Abia State on the extent of utilization of network control strategy for ensuring effective security of data based on years of working experience (11 years and above/6 – 10 years/1-5 years).

Table 2

Summary of one-way Analysis of Variance (ANOVA) on the mean ratings of data managers on the extent of utilization of network control strategy for ensuring effective security of data based on years of working experience

Source of Variance	Sum of Squares	df	Mean Square	F-ratio	P-value	Decision
Between Groups	1.44	2	0.72	1.14	.87	Not Significant
Within Groups	992.34	340	5.14			
Total	993.78	342				

Table 2 shows that f-ratio of 1.14 at 2 and 340 degrees of freedom with a p-value of .87 is greater than the alpha level of .05 (.87 > .05). Since the p–value is greater than the alpha level, the null hypothesis was therefore accepted. This means that there is no significant difference in the mean ratings of data managers on the extent of utilization of network control strategy for ensuring effective security of data in government parastatals in Abia State based on years of working experience.

4. DISCUSSION OF FINDINGS

Findings of this study revealed that network control strategy is utilized to a low extent by employees for ensuring effective security of data in government parastatals in Abia State. This findings could be attributed to lack of/or inadequate data security management skills and competencies among office staff working in government parastatals in Abia State. It could also be that majority of these office employees covered have not received adequate training and re-training programmes on how to effectively handle sensitive organizational data. Additionally, low utilization of network control strategies could be due to negligence and carefree attitude of employees in handling government properties (data inclusive). The findings of this study agrees with that of Olayemi (2014) who revealed that that activities of cybercriminals are the major information/data security challenges facing public organizations in Nigeria. Yusof, Muhammad, Sabarudin and Ghani (2021) underscored the significant impact of data theft on individuals and organisations (government parastatals inclusive since customers' information or data is a precious commodity in today's world. Okunoye, Adebimpe, Omilabu, Olapeju and Longe (2012) earlier observed that most public organizations lack pragmatic data security policies and measures for employees to leverage on. In support, Adelola, Dawson and Batmaz (2015) noted that the Nigerians did not trust the government parastatals to protect their data with any effective legislation or law enforcement, The findings of this study also indicated that there was no significant difference in the mean ratings of data managers on the extent of utilization of network control strategy for ensuring effective security of data in government parastatals in Abia State based on years of working experience. The findings of this study however contrast with the opinion of Chen (2013) that experienced data managers have over the years developed effective strategies for securing their organization's data when compared with the less experienced managers.

5. CONCLUSION

Data are assets and livewire of any organization whether private or public. The survival of any organization depends to a great extent on security of sensitive organizational data. Security breaches or compromise can result to loss or damage of data, leading to legal liability, loss of customer trust or financial losses. This underscores the importance of security of data of government parastatals. The findings of this study revealed that network control strategy is utilized to a low extent for effective security of data in government parastatals in Abia State. Hence, the researchers concluded that there is need for training/re-training of office staff on how to utilize network control strategy to ensure effective security of data in government parastatals in Abia State.

6. RECOMMENDATIONS

Based on the findings of this study, the researchers made the following recommendations:

i. Management of government parastatals in Abia State should organize regular data security training workshops for all their staff to enable them up-data their skills and competencies in utilizing network control strategy for security of organizations' data.
ii. Data managers should carry out regular supervision of office staff to ensure that they are implementing network control strategy in their daily work activities.

REFERENCES

Adelola, T., Dawson, R. & Batmaz, F. (2015). Nigerians' perceptions of personal data protection and privacy.

Al-Awadi, M & Renaud, K. (2016). Success factors in information security implementation in organizations.http://www.semanticscholar.org/6aff/ eddfdifdiadcf737184ffd887602007afod.pdf

Chen, Z. Xiao, N. & Liu, F. (2013). An SSD-based accelerator for directory parsins in storage systems containing massive files. *Peer-to-Peer Net- working and Applications*, *5*(4), 39-40.

Cloud Security Alliance (2012). Top ten big data security and privacy challenges. Retrieved from: http://www.cloudsecurityalliance.org

Federal Republic of Nigeria (2013). *National policy on education*. Abuja: Nigerian Educational Research and Development Council.

Hornby, A. S. (2018). Oxford advanced learner's dictionary. (9th Edition) New York: Oxford University Press.

Ifejika, L. C. (2015). *Career readiness of the office technology and management students in polytechnics in Anambra, Ebonyi and Enugu States, Nigeria.* (Published M.Ed. thesis), University of Nigeria, Nsukka

Kitonga, D. M., Bichanga, W. O. & Muema, B. K. (2016). The role of determining strategic direction on not-for-profit organizational performance in Nairobi County in Kenya. *International Journal of Scientific & Technology Research, 5*(5), 28-32.

Lynch, B. (2022). Data security. Retrieved from: https://www.imperva.com/learn/data-security/data-security/

Okunoye, A., Adebimpe, L. A. Omilabu, A. Olapeju, I. O. & Longe, O. B. (2012). Information security awareness among SMEs in the South Western Nigeria -Significance of factors. *African Journal of Computing & ICT, 5*(5), 184-93.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116-125.

Ponemon Institute (2010). The liability of technology companies for data breaches. The 2010 verizon data breach investigations report, Verizon and the U.S. Secret Service.

Privacy Technical Assistance Center (PTAC) (2015). Identity authentication best practices. Retrieved from: http://ptac.ed.gov

Ray, L. L. (2013). A matrix model for designing and implementing multi-firewall environments. *International Journal of Information Security Science, 2*(4), 119-128.

Sani , A., Mohammed, K. and Aliyu, Z. G. (2017). A review of accounting skills acquisition in business education, enhancing career success. *KIU Journal of Humanities, 2*(2A), 177–183.

Shah, M. H., Ahmed, J. & Soomro, Z. A. (2016). Investigating the identity theft prevention strategies in m-commerce. International Conferences ITS, ICEduTech and STE 2016.

Thompson, J. T., Hertzberg, J. & Sullivan, M. (2011). Social media and its associated risks. Grant Thornton LLP.

Yusof, M. H. A. H. M., Muhammad, K., Sabarudin, S. A., & Ghani, E. K. (2021). Can Internal Control, Rules and Regulations and Technology Adoption influence Bank's Protection of Customers' Data Security? *International Journal of Academic Research in Business and Social Sciences, 11*(9), 1276–1290