Vol 8. No. 1 Issue 2 – May, 2015

African Journal of Computing & ICT

www.ajocict.net

Appropriating Security Assurance Infrastructure and Practices to Counter Data Breaches

[1]D.E. Akpon-Ebiyomare & S. Konyeha
Department of Computer Science
University of Benin, Benin City
E-mails: dorothy.akpon@uniben.edu, [2]susan.konyeha@uniben.edu
[1]Phone: 08023400716

ABSTRACT

Securing an organisation's database should be a thing of concern of all organisations irrespective of size. Databases are among the most targeted organisational assets by hackers and malicious insiders according to a 2014 data breach report. This threat is encountered by both the traditional databases and the big data technologies. Data to any organisation is an asset that needs to be protected from malicious or accidental loss, destruction, disclosure or modification. In this information age, where data are now stored in digital forms and they flow seamlessly between individuals, departments and organisations through various devices, the number of ways that the security of data is threatened has increased. Studies have indicated that in respect of protecting organisations critical data, both technical and non technical strategies are important. As preventive measures, organistions need to have in place effective data security technologies, processes and personnel to monitor, detect, and block threats to sensitive data while in use, in motion or at rest. Fortunately, there are simple steps, internal control and best practices that organisations can implement to counter moves by the various threats from both internal and external sources. Best practices on data security are similar all over the world. This study investigated the data protection and threats detection technologies, processes and security culture of five organisations from both the public and private sectors. The focus of this study was on two of the three major categories of data: data in use (active data stored in databases) and data at rest (archival and backup data in databases). Semi structured interview approach was used to gather data from forty four information technology personnel from five organisations representing the public and private sectors that have adopted information technology to support their organisational processes. The outcome of the study reveal the state of data security infrastructure and the data security management behaviour of the case organisations. It also revealed the factors that threaten the security of organisations data and countermeastures to assure data security.

Keywords: Threats, data security, data-in-use, data-at-rest, security, databases, countermeasure

African Journal of Computing & ICT Reference Format:
D.E. Akpon-Ebiyomare & S. Konyeha (2015): Appropriating Security Assurance Infrastructure and Practices to Counter Data Breaches. Afr J. of Comp & ICTs. Vol 8, No. 1, Issue 1. Pp 77-82

1. INTRODUCTION

A data breach occurs when confidential, protected and sensitive data are potentially exposed to being viewed, copied, transferred, destroyed, change content by unathorised persons. These data include the health status of individuals, credit card or e-payment information, and intellectual property [1]. A Gartner report stated the probability that an organisation will experience data breach is 26%. According to the IBM and Ponemon Institute research report on the 2016 cost of data breach study, there is 29% global increase in total cost of data breach since 2013 [8]. Data and information management are critical aspects of database management. Organisation with high volume of data usually have three types of data: data in motion (on the move through networks within and outside the orgnaisation); data at rest (stored in databases as archives); and data in use (in the desktop for use by employees and clients). These data could be transported throughout an organisation and also outside an organisation by devices such as mobile devices, email, web tools and endpoint devices [4]. Data security management involve technologies, people and processes which provide access to a database.

These security measures that can be put in place to support organisations to manage and protect data from being leaked, modified, copied, deleted, destroyed or transmitted without authorisation [6]. These measures are critical especially for organisations with very sensitive data with long shelve life, like health organisations, financial organisations, and educational institutions. Securing information or data assets of an organisation is the protection of their data asset from unauthorised access, copying, transfer, destruction, use or modification [1]. Organisations with high volume of data usually have three type of data: data in motion (on the move through networks within and outside the orgnanisation); data at rest (stored in databases as archives); and data in use (in the desktop for use by employees and clients) [9]. The transportation of the data is made possible by means of mobile devices, email, web tools and endpoint devices [4]. There are data security measures that support organisations to manage, monitor, detect, and protect data from threats. To secure data against these threats, both technical and non-technical methods are required [2; 10].

2. STATEMENT OF PROBLEM

When the security of such sensitive data is breached, its effect to the organisation is more than financial. Its reputation and brand name is highly affected and it may threaten the existence of the organisation. The reason is that a number of current and potential customers are missed [6; 12]. Data breaches are becoming more frequent and the financial implication is growing. It is important therefore to determine the practices and basic data security infrastructure in the target organisations that contribute to this so as to carry out preventive measures. A number of data security breaches could have been prevented by simple security steps taken by organisations and users of the information system. The top database security threats countermeasures include: key lock and personnel security at entrance; regular backup of files; database scanning; biometric authentication; and encryption of data at rest [11; 4; 10]. The study looked at these security countermeasures and determined the level of compliance by the target organisations.

3. OBJECTIVE OF STUDY

Data security management literature emphasized the importance of focusing on both the technical and non technical aspects that relate to data security management [11]. There are technologies and strategies that preserve the integrity and confidentiality of the data asset of an organisation to an acceptable degree. Their absence could expose the data of organisation to internal and external threats and attacks. The objective of this study is to investigate the infrastructure, strategies and culture in place at the targeted organisations to counter data security threats. The study is focused on data-in-use and data-at-rest. The technical security mechanisms are the technologies that provide services like digital signatures and fire walls, while the non technical services are the practices and values of the organisations in ensuring data security [11].

Therefore the study examined the presence of the basic attributes of data security that is able to put under control the risks faced by an organisation's data and information. The category of data under investigation by the study is data-at-rest and data-in-use.

4. MATERIALS AND METHODS

A total of twenty five information system professionals from five organisations participated in the survey. The organisations were from both the public and private sector representing education, health, manufacturing, sales and distribution. The organisations were either medium scale or large scale The study used face-to-face semi-structured interview method to gather data from the respondents of over a period of eight weeks. In addition, observation was used to investigate the culture as well as assumptions of the employee as it related to security. The study used exploratory case study approach to elicit information. The interviews took place mostly at the organisation's premises while telephone interviews were conducted to clarify some issues. The interview questions were in a Likert scale format. Each interview lasted for about 30 minutes and the question categories included: demographic information of respondents; the security technologies in place, strategies that prevent data breach and the security culture of the people working with the information system. The question covered both the technical and non technical issues and how the security technologies were implemented. The analysis of the data enabled the determination of the level of data security management practices in place and the factors that affect the implementation of security infrastructure. The population selected for this study, is made up database administrators, data managers and data custodians whose responsibility include ensuring the integrity of the master database content. The data collected were coded and entered into the SPSS (Statistical Package for Social Sciences) for Windows for analysis.

5. ANALYSIS AND RESULTS

The result of the analysis are reported below. Table 1 provides an overview of the case organisation.

Table 1: Overview of case organisations

S/N	CASE	Case Description	Ownership	Respondents per case	%
1	A	Electricity distribution Coy	Private	4	9
2	B	Federal Higher Institution	Public	22	50
3	C	Manufacturing/Sales	Private	4	9
4	D	Population Commission	Public	6	10
5	E	Private Higher Institution	Private	10	23
		TOTAL		44	100

Table 2: Information Technology Practitioners That Participated

S/N	**Participants Description**	**Work Competence**	Num of Respondent	%
1	Database administrator	database management and computer training	6	14
2	Systems analyst / programmer	Database management, records processing and data capture supervision,.	24	54
3	Network Engineer	Network / database management	10	23
4	Data entry /capture supervisor	Data entry/capture supervision	4	9
	Total		44	100

5.1 Technologies: Physical and electronic Security

Access control systems prevent intruders from getting access to the information system that house the data-in-use or the storage system used as backup for the data-at-rest. In many cases, the presence of physical security measures act as deterrents to potential data criminals as the possibility of being caught is a deterrent to many. Table 3 show the availability of basic access control systems in the target organisations.

Table 3: Availability Of Basic Access Control Mechanism

S/N	**Organisation**	**Security personnel at entrance**	**Key Lock at entrance**	**biometric authentication**	**keycard locks**	**Security camera**	**Security light**	**24 Hour Access to Light**
1	A	Yes	Yes	No	No	No	Yes	No
2	B	Yes	Yes	Partially	Partially	Partially	Yes	No
3	C	Yes	Yes	No	No	No	Yes	No
4	D	Yes	Yes	No	No	No	Yes	No
5	E	Yes	Yes	No	No	No	Yes	No

All case organisations have security personnel and mechanical key locks at entrance as the common physical access control mechanism in their organisations. None of them fully use biometric technology like facial recognition, fingerprint, retinal scan, iris recognition, voice, and hand geometry to support the use of physical access control technology. Security camera is a very basic form of security control which can record access of persons in and out of a secure place. The organisations do not have it in place except for the public higher institution and this is partial. The issue of constant power failure contribute to poor data security. Some of the devices depend on electric power.

Table 4 shows the result of the data security countermeasures in place in the organisations based on three categories of security threats: Organisation security measure, Infrastructure, employee security culture in place at case organisations studied.

Table 4: State Of Data Security Countermeasure Taken By Each Organisation.

S/N	CATEGORY	DATA PROTECTION ATTRIBUTES	RATINGS					
			Disagree/ Percentage		Undecided / %		Agree/ %	
1	Security Measures	My organization's current security activities are enough to stop a targeted attack (or Advanced Persistent Threat) or a hacker	38	86%	0	0%	6	14%
2		We manage off-line data-bearing devices including their safe disposal	30	68%	10	23%	4	1%
3		We train and educate system users about IT security policies and procedures	30	68%	4	9%	10	23%
4		Encryption of data at rest	36	81%	4	9%	4	9%
5	Security Infrastructure	My organization's security infrastructure needs to focus on data-centric (inside-out) security with sensitive or confidential data being the main element.	0	0%	6	14%	38	86%
6		In my organization, data Intelligence that identifies the "who, what, when and how" data is accessed is a high data protection priority.	30	68%	10	23%	4	9%
7		In my organization, data Intelligence that identifies the "who, what, when and how" data is accessed is a high data protection priority.	18	41%	6	14%	20	45%
8	Employee Data Security Culture	Employees routinely back-up information contained on their computer	34	77%	4	9%	6	14%
9		Employees do not connect their computer to the Internet through an insecure wireless network.	18	41%	20	45%	6	14%
10		Employees remove or delete information contained on the computer when no longer necessary.	36	81%	2	5%	6	14%
10		Employees immediately notify their organization when a computer is lost or stolen.	4	9%	0	0%	40	91%

6. FINDINGS AND DISCUSSION

This study findings indicates that: there is general lack of wide understanding of the data security habits, and control by employees in the organisations studied. Inadequate training on data security may be partly responsible for this, as the study showed that.

i. There is generally no standard strategy in place by the organisations to ensure data security.
ii. Employees have the impression that ensuring the security of data is the responsibility of management.
iii. There no documented policy in place for regular file backups. Backups are carried at the convenience of the employee in charge. This could result in loss of critical data without provision for restore when the master data is corrupted or lost. The responses of the employees indicating that 77% of respondents do not routinely back-up information contained on their computer.
iv. 81% of respondents do not remove or delete information contained on the computer when no longer necessary is an indication that they do not fully understand the part they need to play in ensuring security.
v. For employees to see security as also their responsibility, it is necessary for management of the respective organisations to sensitize information technology on simple steps to take to protect the organisation's data assets.
vi. 81% of the respondents do not practice data encryption for data-at-rest. This exposes critical data to hackers.
vii. Organisations do not properly dispose of data assets that are no longer needed. This is evidenced by the 68% responses that unusable data assets are stored and later thrown away and not properly disposed of.
viii. Programmers or data capture personnel with no formal training on data security management.
ix. The employees need to understand data security policies. This can be achieved by organising regular training on data security and the policies of the organisation.

Organisations need to carry out review of their data environment in order to identify where their sensitive data is at risk. This include knowing where all sensitive data in the organisation that at rest live and the level of protection that they have. For all the organisations, the security of data at rest is porous. Data at rest for all the organisations have very minimum security when compared to data in use. According to [2], behavioural security is the key to security assurance. The findings from the study indicates that the organisations personnel unintentionally create data exposure by their attitude to security (Table 4). None of the organisations adequately practice encryption of their data at rest.

The most common form of security is key lock and security personnel at entrance of the department to prevent physical access to where the data lives (cabinet, drawers or data store room). Regular backups is one major data protection measure that is cheap and if personnel in charge make a habit of it, would save organisations both financial and credibility issues. The personnel at the organisation fail in this aspect and their explanation was heavy work load leaving them with little time for other very critical activity of file backup. The design and implementation of the information security management system (ISMS) would ensure adequate security of organisations data asset.

The behaviour of personnel need to redirected towards security. Training of personnel on the need and consequences of data breaches is very important as acquisition of security technologies alone will not provide needed security without the dedication of the personnel who use the technology. There should be laid down procedure for when a staff member is transferred or leaves the organisation and also when a new one comes in regarding setting them up and disabling their priviledges.

8. CONCLUSION

Securing data and information assets need not be expensive. There are basic activities and strategies that organisations in Nigeria can put in place to ensure security of their data assets. Successfully managing information assets require the involvement of technologies, people and processes. One common and basic need of the organisations is data security personnel with the knowledge and experience to manage and implement information security best practices. The findings indicate a shortage of this category of information technology personnel in all the organisations under study. There should be documented procedure on how to prevent data breaches, what to do when it occurs and the consequences on the personnel through whom the breach occurred due to his negligence. Organisation need to be very aware of the privileges granted to employees, ensuring that they do not get more privilege than they require to carry out their tasks. When duties change for an employee, the previous privilege need to be withdrawn instead of adding it to privilege required for the new task.

9. RECOMMENDATION FOR FURTHER STUDIES

One possibility for future research in this area of study is determining the level of cultural influence on the security of organisation's data assets. Another study could be carried out with more sample size involving more organisations. Significant insight could be gained if the result of this study is compared with outcome from organisations in a more developed environment.

REFERENCES

[1] Allen, J.H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley.

[2] Dhillon G. and Torkzadeh (2006). Value-focused assessment of information system security in organisations. Information System Journal Vol. 16:293-314.

[3] ISO/IEC (2013). The International Standards ISO/IEC. Retrieved September 10, 2014.

[4] May L. and Lane T. (2006). A Model For Improving E-security in Australian Universities. Journal of Theoretical and Applied Electronic Commerce Research. 1(2) 90-96.

[5] Muller, H., and Freytag, J.C. (2003). Problems, Methods, and Challenges in Comprehensive Data Cleansing. *ech. Rep*, HUB-1B-164.

[6] Peltier, T.R. (2002). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications.

[7] Driscoll T. and Dolden B. (1997). Computer Studies and Information Technology. Macmillan education Ltd: London and Oxford.

[8] Richard A., Riley R.A., Pearson T,. and Smith M.C., (2016). The Effect of Identity Fraud to Financial Services Organizations: Costs, Losses, Resource Requirements and Best Practices.

[9] Setia, P., Venkatesh, V., and Joglekar, S. (2013). "Leveraging Digital Technologies: How Information Quality Leads to Localized Capabilities and Customer Service Performance." *MIS Quarterly*, 37(2), 565-590.

[10] Siponen and Oinas-Kukkonen (2007). A review of information security issues and respective research contributions". SIGMIS Database. 38 (1). 60-80.

[11] Von Solms B. (2006). Information Security:- The Forth Wave - Computers vs Security. 25(3) 165-168.

[12] Vaziri Y., Reza. M. And Mehran. (2012). “Towards a Practical State Reconstruction for Data Quality Methodologies: A Customized List of Dimensions". Second International Conference on Computer Science, Engineering and Applications (ICCSEA-2012).