THE RISK OF DATA LEAKAGES AS DATA GROWS IN INFORMATION TECHNOLOGY-DRIVEN TERTIARY EDUCATION INSTITUTIONS

Wahab Akanni Adeniyi & Johnson. O. Fatokun[*]
Department of Mathematical Sciences, Anchor University Lagos
*e-mail: jfatokun@aul.edu.ng

ABSTRACT

Expansion is a major goal for educational institutions and Information Technology is readily useful for its drive. In a bid to achieve this goal, IT assets are added and more data are generated. Data growth is not just uncontrollable but that the rate is alarming. Data then become an important asset for running the day-to-day educational activities such as updating students' records, examination questions, result transcripts, payment records, staff salaries, proprietary information and strategic decisions. They underscore the importance of data. Hence, the need to safely keep data from leakage. Data leakage has continued to be a source of worry to all users because they all need it in one form or the other. For this reason, university management are often faced with the challenge of preventing data leakage while being processed, transmitted, stored or retrieved for specific purposes. While most existing works address detection of data leakage, this paper presents a practical approach to prevent leakage as data generation grows with other IT assets in the tertiary institutions.

Keywords: Risk, IT assets, Data Leakage, Data growth, vulnerability and data integrity.

1.0 Introduction

Information security issue is the most important one in using Internet and it becomes more crucial while implementing the Internet in the tertiary educational sector. This research revealed a lot of risks and threats to the security of information which are increasing day by day. The demand for high security in safekeeping of educational services create both challenges and new day-to-day opportunities. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. Tertiary institutions, which are basically post-secondary education, protect their information by instituting a security process. This process involves identifying risks and forming an appropriate strategy to manage the risks by assessing and analyzing them, implement the strategy, test the implementation and monitor the environment to control the risks. Information security can be enhanced by Information Security Risk Assessment, Strategy, Controls, Implementation, Process Monitoring and Updating. A major threat

*This work is supported by Natural Science Foundation of China under number 11761073.
[†] Corresponding author: Yang-hong Tao, E-mail: taoyanghong12@126.com

to educational institutions is data leakage.

Digital world has continued to grow at an alarming rate. As the growth continues so are the gadgets used in carrying out digital activities. There is also a positive correlation between IT assets and data generated by them. All institutions, irrespective of their sizes, need to understand their data, information and information assets before they can adequately protect them (Mozyenterprise, 2015 and National Archives, 2017). Data leakage can be seen to have occurred when restricted data or information falls into the hands of wrong persons. This may be in hard or soft copies (Baby, A. and Krishnan, H., 2017). The risk of data leakage is not abated even in today's world, where paper usage is fast reducing and various gadgets are involved in data processing. These include institution-owned and personal devices especially where bring your own device (BYOD) is allowed among employees and students. Thus, institutions stand a risk of data leakage through these devices. For the purpose of this paper, IT assets are described as data, information and systems – software or hardware – directly or indirectly owned and used for day-to-day activities by an institution. The risk may be reduced where such IT assets may be more manageable, compared to when they are in large numbers, but does not take away the fact that all organizations have the likelihood of data leakage.

2.0 Possible sources of data leakage in IT-driven tertiary institutions

There are various means of losing data some of which are considered in this section. For instance, commendable expenses are incurred on storage to ensure that adequate backups are taken to prevent data loss. Some institutions even go as far as adopting redundant array of inexpensive disks (RAID) level6 to ensure data are replicated as often as they are generated. There are other means of losing data apart from failure at storage. These include: fire, theft of disk, virus and natural disasters such as tsunamis and tremors. While considerable efforts and progress are made in reducing data loss not so much is noticed with data loss. This becomes more worrisome in big data. There are major avenues through which data leakage can occur through various degrees of unauthorized access.

From previous research work, it was discovered that despite the security policies, procedures, and tools currently in place, employees around the world are engaging in risky behaviors that put corporate and personal data at risk. Employee behaviors included:

- **Unauthorized application use:** 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies' data loss incidents.
- **Misuse of corporate computers**: 44 percent of employees share work devices with others without supervision.
- **Unauthorized physical and network access:** 39 percent of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

● **Remote worker security:** 46 percent of employees admitted to transferring files between work and personal computers when working from home.

● **Misuse of passwords:** 18 percent of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy. This is more common among students of tertiary intuitions in Africa.

To reduce data leakage, businesses must integrate security into the corporate culture and consistently evaluate the risks of every interaction with networks, devices, applications, data, and of course, other users.

3.0 Description of Unauthorized Access

An access to an IT resource can be described as unauthorized when one is getting to use such resources without consent or permission of the owner (Morgan, L., 2015). It can be physical or logical from a staff, an ex-staff, a student or a third party such as a vendor or a service provider who assumed an access right that was not legitimately assign. Unauthorized access can be gained in four main ways:

3.1 Theft

Theft can occur through outright stealing of a storage media. When this happens, information is not only lost but leakage of such details into wrong hands may result. For instance, a storage device storing examination questions that is stolen before the assessment day. There is need to checkmate this.

3.2 Hacking

Hacking involves illegally accessing an information even where security is in place. It can be in form of a brute force. Through hacking, an unauthorized user may gain access to information as if they were never protected. When any system is hacked there is a risk of exposure.

3.3 Inadvertent Disclosure

Sometimes, information may not be intentionally disclosed. Staff of organization may be deceived into giving out essential details which they would not have done ordinarily. It may be through social engineering or improper disclosure of waste bin.

3.4 Inside-related Disclosure

At some other time, there can be intentional disclosure of details by disgruntled staff who felt unhappy for what the institution did or failed to do. By way of paying back, disgruntled staff may give away confidential details such as an intellectual property or a trade secret to a third party. The latter may then utilize such details to outwit its competitor.

4.0 Impact of data leakage

The impact of data leakage can be so severe. The following are some of the effects of leakage of data on an organization:

4.1 Reputational damage

Concepts such as reputation, image, and goodwill denote the general standing of organizations among their peers (Shenkar, O. and Yuchtman-Yaar, E. 1997). Leakage of data can damage the reputation of an organization that has been built over time. Inability to produce information that should be readily available can paint a complete negative picture of an organization.

4.2 Loss of competitive edge

When data is lost, an institution may not be able to immediately meet the needs of its customers nor respond to the competitive challenges thrown at its peers. Customers may be compelled to try a competitor that may prove reliable in meeting their needs thereby losing the customers to other players in the market.

4.3 Litigation cost

Data leakage may get into a wrong hand. For instance, where a backup tape containing some personal details (like health status or bank details) is lost and made public by a third party may lead to litigation. An aggrieved customer may decide to engage the institution in a legal battle.

4.4 Fraud and security breaches

Lost data may lead to fraud. A typical example is gaining access to a file containing security details of an institution's staff by a fraudster. Such files could have been stolen through hacking, key loggers or other less sophisticated means like social engineering. The stolen can be used to perpetrate frauds.

5 Measuring Data Leakage

The task of measuring data leakage is such a difficult one. It involves combination of money, time and reduced productivity (Smith, O. 2015). Sometimes, one may want to see data leakage in financial terms only. While this can be true, especially when considering the amount involved in replacing lost the systems or media where leakage data reside, it should be noted also that invaluable time is involved in capturing. The impact can as well be extended to leakage of productivity. An aggregate of these factors can give an estimate of measurement of data leakage by way of attaching monetary values to each. For instance, if there is a data leakage occasioned by a natural disaster (say, flood) that swept the computer systems which cost ₦50,000,000. Assuming the data not backed up will take three hours to be recaptured from source documents by seven staff with hourly wages of ₦1500 and verified by two officers with wages of ₦2,500 per hour for four hours. Barring some other unquantifiable impacts like reputational damage or litigation that can go as high even as to sinking the entire day-to-day, the organization must have lost (₦50,000,000) + (₦1500*3*7) + (₦2500*4*3). This is N50,033,150 all things being equal.

6 Cases of Data Leakages in Tertiary Institutions

Data leakage has been on the increase in recent time. Some specific reported cases are referenced here for review: According to Cortez, B. (2017), there was a more than 100% increase in data breaches on education sector during the first half of 2017 when compared to the same period in the previous year. In education sector alone, about 13% of the total successful attacks were observed which ranked third behind the financial and healthcare sectors for obvious reasons. Coleman and Purcell (2015) also opined that data breaches are on the increase in institutions of higher learning. The further observed that 36% of breaches were committed by hacking or malware, 30% by unintended disclosure, and 17% by portable device breaches. Some specific reported cases are referenced here for review:

Bearak (2018) held that all institutions will be attacked. However, the time when it would occur may not be known. He stressed that higher education institutions are major targets for intruding hackers. University at Buffalo was breached and more 2,500 details meant for students, ex-students and staff. According to TrendMicro (2108), there were data breaches in the University of Maryland that compromised the details of both staff and students. These include: names, birth dates, university ID numbers, and Social Security numbers.

TrendMicro (2108) stated that the University of Greenwich got essential details of students compromised through an unsecured site.

7 Practical methods of preventing data leakage

Having reviewed the major impacts that data leakage can have on organizations, there is a need for a real-world approach to reduce its occurrence. Several attempts have been made by authors to address data leakage using Watermarking (Kadu, R. and Gadicha, V., 2017), Steganography (Jain, M. and Lenka, S., 2016) and Data Allocation (Tuccano, G. et al., 2015). While these methods can reduce leakage, they are mostly related to discovering alterations. They are of detection. Today, leakage may not be limited to only copying or altering the original information. A whole lot of havoc may be wreaked when an unauthorized person views some proprietary information and uses same to his own advantage. This action may go undetected since to alteration is observed. Thus, this paper proposes a strong encryption mechanism that makes the content of data in any state private and confidential by not allowing an unauthorized person an access to make a meaning out of it.

7.1 Implementation of Data Leakage Prevention Through Cryptography

Cryptography is a way of concealing information by writing so that not everyone can read its content with a view to making meaningful interpretation from it. It is also known as encryption. Encryption process involves converting a plain to a cypher text. When this is done, such data is said to have been encrypted whereas to read correctly, it has to be converted back to plain text otherwise known as decryption by using key encryption and decryption keys respectively. The primary purpose of cryptography is to maintain privacy as well as confidentiality**.** Algorithms are involved in the encryption process with varying degrees of complexity. Encryption algorithms can be Secret Key

Cryptography, Public Key Cryptography or Hash Functions. While encryption, and indeed Public Key Cryptography, is highly recommended for data leakage prevention in this paper, some other compensating controls should be in place. Once a policy is in place, implementation of data leakage prevention can then commence by the Steering Committee in order to decide on the strategy to be adopted. For instance, for network, an end-to-end implementation may be better. In stored state, all discs and devices should be encrypted to prevent leakage. Even when stolen or lost, the content can still be unreadable by unauthorized persons. For implementation, five stages are prescribed as explained below:

Stage 1: Establishment of Data Leakage Prevention Framework

The board of an organization has the role of designing appropriate framework that will prevent data leakage. As part of the consideration, training of staff, signing of a non-disclosure agreement, perimeter coverage as periodic review of access control. This will also guide on acquisition and usage of mobile devices, While BYOD is a good idea that allows for flexibility in working away from offices, management must ensure that all staff adhere to the best practice in its usage. This may include links through secure connections, encryption of the devices and awareness on safe keep among others. The framework will go a long way to prevent data leakage if it well designed and implemented.

Stage 2: Awareness

It is very important to run a regular campaign on information security to create necessary awareness such that individual's roles, responsibilities and limitations are properly communicated to all stakeholders – staff, vendors and customers. Such campaigns should detail key tips on how (and how not) to handle data or information of the organization as well as the next thing to do where a data leakage occurs.

Stage 3: Disposal Policy and Procedure

Every organization must have a policy on disposal of obsolete items. The way to treat an obsolete IT asset should be documented to guide on how such assets should be treated. Policy and procedure should be in place to ensure that there is no deliberate or inadvertent erasure or deletion while rotating disks. Such items containing sensitive or confidential details may have to be burnt or destroyed under a close supervision after proper review and confirmation the intended disc is the one disposed.

Stage 4: Regular Review of Access

Regular access review of access right should be done. This will help to suspend unauthorized profile created. Where this fails, disgruntled ex-staff's or hacker's accesses can delete valuable data because he was not disabled on the system after exiting.

Stage 5: Periodic Vulnerability Assessment and Application of Patches

Viruses can lead to data leakage. Therefore, antivirus should be current. Periodic vulnerability assessment can also help to detect various threats to data and application of updated patches will reduce loss of data.

8 CONCLUSION

Data occupies a pivotal role in the activities of an organization. Thus, an organization needs to do all within its capability to prevent data leakage, in whatever form. While due registration of all communicating devices within the network is necessary, encryption of those devices must also be taken care of to address data leakage issues.

REFERENCES

1. Baby, A. and Krishnan, H. (2017). A literature survey on data leak detection and prevention methods. International Journal of Advanced Research in Computer Science. Vol. 8 No. 5
2. Bearak, S. (2018). Data breach & technology, identity & privacy, personal. www.identityforce.com
3. CISCO (2008): Data Leakage Worldwide: Common Risks and Mistakes Employees Make. White Paper of CISCO Systems Inc.
4. Coleman, L. and Purcell, B. (2015). Data breaches in higher education. Journal of Business Cases and Applications. Volume 15, December 2015
5. Computer Security Institute. 2000 Computer Crime and Security Survey, 2000 (available from http://www.gocsi.com; accessed March 2000).
6. Cortez, M. B. (2017). Education sector data breaches skyrocket in 2017. www.edtechmagazine.com
7. Information Security Industry Survey. Information Security Magazine, July 1999 (available at http://www.infosecuritymag.com; accessed September 1999).
8. Jain, M. and Lenka, S. (2016). A review on data leakage prevention using image steganography. International Journal of Computer Science Engineering. Vol. 5 No. 02
9. Kadu, R. and Gadicha, V. (2017). Review on securing data by using data leakage prevention and detection. International journal on recent and innovation trends in computing and communication. Vol. 5 issue 5 pp 731-735
10. Morgan, L. (2015). Hacking Vs unauthorized access. www.itgovernance.co.uk
11. Mozyenterprise (2015). Data leakage: understanding the causes and costs. url:www.mozy.com.
12. National Archives (2017). Identifying information assets and day-to-day requirements.www.nationalarchives.gov.uk
13. Shenkar, O. and Yuchtman-Yaar, E. (1997). Human relations. www.doi.org
14. Smith, O. (2015). The real cost of data leakage and how to prevent it. www.techgenix.com
15. TrendMicro (2018). Data breach 101. www.trendmicro.com
16. Tuccano, G., Kotadiya, H., Bhat, V., Fernandes, R. and Panchal, A. (2015). A

survey on data leakage detection. International Journal of Engineering Research and Applications. Vol. 5, issue 4

17. Vishal R. Ambhire1 and Prakash S. Teltumde (2011): Information Security in Banking and Financial Industry. International Journal of Computational Engineering & Management, Vol. 14, October 2011 ISSN (Online): 2230-7893. www.IJCEM.org