IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Security of Critical Data in Universities.

**Authors**

1) Mr. Stephen Ochieng' Oguta: Kisii University
2) Dr. Charles Ochieng' Oguk: Rongo University

## ABSTRACT

Organizational critical data is essential for her core operations and stability of financial operations. Maintaining security of critical data in organizations has been scholarly and industrially emphasized in many cases. Nevertheless, studies focusing on highlighting university critical data and implementation of the key elements of the data security in institutions of higher learning is still inadequate. This study was conducted within computing context of universities in Kenya, where it aimed at investigating the critical data and the levels of implementation of key aspects of data security. Questionnaires were used for data collection from staff members who were mainly sectional heads of user departments and information systems' administrators. The data analysis produced statistical values needed to address the study objectives. Results showed that academic and financal related data were considered as critical data in the university. Furthermore, it was found that many universities have fairly implemented vital aspects of data security. However, in some universities, data security practices were found to be inadequate. For example, use of portable external storage devices to tranfer files between computers and malware menace. Therefore, it is recommended that universities ought to ensure security practices for critical data for better information systems security management. The study also recommends that IT security policies should include critical data security for a given organization.

**Keywords:** data security, critical data, data back-up, data retrieval, data encryption, information systems security, user priviledge, ICT security.

## INTRODUCTION

### Critical Data

Critical data is defined as the data that is crucial to success of a specific business or organization, since such data is required to get the main job done, (Newswire, 2018). The identification of organizational data and classification of critical data elements is an information governance practice that improves revenue and product quality, (Rabah, 2018). In view of the researcher, critical data usually encompasses data and files around the core mandate of an organization as well as her financial data, (The Author, 2020). It implies that proper implementation of critical data elements helps to prevent disruption of an organization's core business and loss of revenue; a view supported by Rabah, Research, & Nairobi (2018). Equally, proper governance of organization critical data can maximize customer satisfaction, revenue, and ensure operational cost-efficiency (Sun, Cegielski, Jia, & Hall, 2018).

According to Selwyn (2007), wide spread adoption of information technology has created more efficiency in handling academic and administrative data at the levels of file generation, storage, processing, caching, long haul transit and transfers through local area networks.

Apart from user originated data through file generation, automation systems like student registration systems, student finances and examinations systems that are used in the universities are the major sources of data (Ndung'u 2015). ERP being an automation tool, generates so much data in electronic form, and at the same time, resides on the university operating network, hence access into it must be controlled, to guarantee data integrity (Galliers, and Leidner, 2014). Other data resources are generated by automated learning platforms within the universities. For instance, according to Tarus, Gichoya and Muumbo (2015), e-learning – a teaching and learning platform of information technology enabled by the internet, has been adopted in the universities in Kenya to successfully reduce financial and geographical barriers to higher education. The much data in the university databases has created automation and efficiency in universities to an extent that use of database systems can only continue therein, (Oguk, Karie & Rabah 2017).

### Security of critical data

Despite the major success of efficiency through automation, Luambano and Nawe (2004) noted information security concerns as student exam management systems, financial and payment systems in universities are mostly web-based and hence the data generated remain accessible not only through the internet, but also via mobile systems. Regarding information systems security, Sridhar, & Govindarasu, (2014) showed that data storage, use and transfer through computer networks expose the university's data to cyber-criminals and other threat agents, a view held as well by has Oguk, Karie & Rabah (2017). Luambano and Nawe (2004) reviewed that data security is built up by features like; encryption of data files, users' restrictions to data resources, data backups, data restoration, malware control on systems holding data, hot site, availability of critical servers and applications. While the studies underscored the importance of data security in universities, the implementation levels of the features of data security has not received much scholarly attention.

## Statement of the Problem

While security of critical data in vital in any organization, universities in Kenya and higher institutions of learning around the world experience various information system security challenges which compromise the organizational information assurance. Many studies including Luambano and Nawe (2004) have highlighted the key aspects of organizational critical data security that if properly implemented, can provide security assurance to data. However, related contemporary scholarly works have not adequately encompassed the implementation levels of the data security key aspects. There is a need to assess both the critical data in universities and the implementation levels of major elements of data security within universities in Kenya.

## Objectives

i. To determine the critical data in universities in Kenya

ii. To assess the levels of implementation of critical data in universities in Kenya

## LITERATURE REVIEW

### Data security

While analyzing data security the United Arab Emiates, Saleh and Bakry (2008) defined data security as the protective measures that are implemented in an information systems to prevent unauthorized access to computer data, files, databases and websites, thus safeguarding data against corruption, manipulation and loss. It noted that while features that directly address data security play a vital role in information security management, the methods used lack the data security features like encryption. The study claimed that information security management within universities could be more effective if data security is given high priority in the IT security management program.

In the US, Tomlinson (2016) noted that a hacker broke into computer system of a university in California, and compromised security of data associated with over 80,000 stakeholders - mainly students and faculty members. Tomlinson demonstrated that despite the administrator's knowledge of data encryption requirement in the database, the data security technology was lacking, a situation that was attributed to the vulnerability observed. It contend, therefore, that there should be a check-list indicating the required data security features in IT security management program, to help remind administrators of the necessary tools and practices as a way of improving data security.

Ismail and Zainab (2011) conducted an assessment survey on information systems security in Malaysian's special and public libraries with an aim of establishing information technology security status in the libraries. The study only considered the principle of least privilege, good backup policies and data recovery procedures to ensure information systems' security. In contrast with the study conducted within Malaysian libraries, Casey (2011) suggested that data security consideration should include data encryption at minimum to qualify as a major element of information technology security. On the other hand, Grama (2014) conducted a research to analyze data breaches attributed to institutions of higher education in the United States. Gama found that the number of data security breaches is much more than that recorded; a view held by (Sandler, Derr, & Wallach, 2008 & (Makori & Oenga, 2015). The study considered the adverse effects that the institutions suffer at the height of data integrity breaches and suggested that data security management should include users' restrictions and malware control, besides the features highlighted in the abovementioned studies. Nevertheless, Grama supported the consideration of data security elements in the aforementioned studies.

In Tanzania, Luambano and Nawe (2004) pinpointed that student exam management and finance management systems, being web-based, the data therein remains accessible not only through the internet, but also via mobile systems, that makes the university data vulnerable to hackers. Blank (2015) reviewed a case where more than 418 students managed to breach a university's IT security in Uganda and altered their marks to better grades. Sridhar and Govindarasu (2014) supported this view and showed that data storage, use and transfer through computer networks expose the university's data to cyber-criminals and other threat agents. Also, Sadeghi, Wachsmann and Waidner (2015) agreed with the studies and further showed that hackers associated with students are lured by information rich networks where they tamper with university's IT systems to adjust grades and fee balances in their favor.

In Kenya, Mulwa (2012) noted increased dependence on information technology by universities in Kenya against heightened information security breaches, and recommended high security control practices to safeguard university data. The study found that in universities in Kenya, students, employees, contractors affect security of information systems. In agreement with this, Deloitte East Africa (2011) revealed that in Kenya, information security breaches have resulted to changes in information systems security management practices, with proactive safeguard measures gradually being adopted. It claimed that the shifts in data security management now focuses on people, especially the users and database managers, who are viewed as the weakest points within the chain of information security system.

Still in Kenya, Okuku, Renaud, and Valeriano (2015) showed that there is need to consider availability of critical servers and applications to ensure data security. The study showed that people are involved extensively in data security management, thus the people constitute elementary points of data security that should be considered to ensure effective information security management program. In addition, Veseli (2011) justified the need to incorporate not only the people, but also data back-up, malware control and user-groups as effective measures for implementing information systems security in universities. Kimwele, Mwangi and Kimani (2011) stressed those users' restrictions to data resources and systems' back-up should be considered in university IT security management program, by setting up user-groups and alternative places for data recovery in case of disaster, which is in support of position taken by Veseli.

In a synopsis, the foregoing studies stress the importance of data security management control practices along the features of data security in the management of information systems' security. In highlighting the features of data security, they studies concur that sub-elements of data security should include: encryption of data files, users' restrictions to data resources, data backups, data restoration, malware control on systems holding data, hot site, availability of critical servers and applications.

The studies pinpointed the aspects of data security that should be considered in estimating data security in an organization and justified the need to properly implement them. However, the studies neither highlighted the critical data, nor did they delve into the levels of implementation of the key aspects of data security in the organizations where research studies were conducted.

## RESEARCH METHODS

### Research design

Mixed sampling approach was adopted in this study. After stratifying the institutions into public and private universities, ten percent random sampling was applied on each strata resulting into seven universities; four being private and three being public universities. Considering thirteen (13) information systems' operational areas (as supported scholarly) purposive sampling was further applied in seven universities, targeting information rich respondents: mainly heads of information systems' user departments and ICT personnel. The operation areas included: IT leadership, Systems administration, Network administration, Security administration, Data-Base administration, Students' finance, Students registration, Examinations, human resources, Internal Audit, University Library, Computer Laboratory and Students Leadership. The sampling produced a total sample size was (13 x 7 = 91 respondents), as drawn in the table below.

*Table showing the sample size*

| Operation Areas | sampled universities | Total |
|---|---|---|
| 13 | 7 | 91 |

Data was drawn from the respondents using well designed questionnaires to address each objective. The questionnaire was designed to include both open ended and closed ended questions. Data analysis was done to obtain pertinent statistical values addressing the given objectives of the study.

## RESULTS AND DISCUSSION

Data security control practices in a university, for example: encryption, back-ups and restoration are necessary in an organization, (Bulgurcu, Cavusoglu & Benbasat 2010). In addressing the first objective, the study further found out that academic and financial information were the most valued in the universities in Kenya at 33 percent and 37 percent respectively. Thus, 70 percent of universities attach great value to academic and financial information systems. This supports the Mahnic, Uratnik and Zabkar, (2002) study among the Slovenian universities that showed academic and financial information systems had much high levels of security as compared to other information systems within the university. Ndung'u 2015 and Casey (2011) noted that students and university personnel do compromise mainly academic and financial systems for their selfish interests. It was found that 62 percent of those sampled have lost data within the system, and which they successfully recover.

University has different types of data. Apart from data originated by the user through file generation, automation systems like student registration systems, ERP (enterprise resource planning), student finances and examinations systems are major sources of data, (Ndung'u 2015). According to Selwyn (2007), data classification is very important in determining the most critical data, and prioritizing security appliances' investment approach to apply. The findings in this research showed that 64 percent of the respondents confirmed that there is data classification in their universities, while 76 percent confirmed that they prevent data leak in their systems. The findings agree with Galliers and Leidner (2014) adding that data classification controls access, reduces data leak, guarantees data integrity and is applicable in most universities and other learning institutions.

In addressing objective two, the study showed that up to 60 percent of the universities successfully back-up their data, while 46 percent retrieve their data effectively after successful back-up. However, only 32 percent of the universities conduct full system back-up while 68 percent of the universities only do simple file back-up. Data security continues to suffer from malware attack that compromises both data integrity as well as availability. For instance, Eira and Rodrigues (2009) showed that universities' networks are frequent sources of malware. The current study found that 64 percent of the universities do not effectively control malware in their systems. This is because up to 48 percent of the respondents admitted unavailability of critical servers and applications due to malware attack.

Further, 49 percent of the users admitted that there is no control on transferring data through portable external storage media like flash - disks and memory cards. This finding concur with Sandvik (2016), that malware spreads fast through such portable devices and this causes multiple losses to information resources, thus rendering information systems unavailable in institutions. The use of external portable storage media contributes so much to malware transfer from one computer system to another, and could be a major concern for data security within universities, Ismail and Zainab (2011). This study found that use of portable devices remains un-controlled within 48.9 percent of the universities in Kenya. The access to the university server room is much restricted in the universities, as 60 percent of the respondents indicated that it is very difficult, as over 90 of the respondents showing that it is difficult. Further, only 47 percent of the universities operate on encrypted files and folders, while 53 percent do not.

Data back-up helps in restoring operations in the event that primary computing data sources cannot be accessed. System back-up considers not only the data back-up, but also the entire application and repositories associated with the data. This is usually more reliable than ordinary data back-up since the secondary site acts as a hot site. The study found out that 76 percent of the respondents sampled from the universities conduct regular and automated data and systems back-up. This is consistent with findings by Ismail and Zainab, (2011) study on Malaysian's special and public libraries that good backup policies and recovery procedures ensure information system's security.

**Summary, conclusion and recommendation**

Data security control practices in a university include encryption, back-ups and restoration. Universities conduct data classification, wherein academic data and financial data were found to be the critical data for the universities. While the universities in Kenya fairly implement data security, higher levels of compliance is still needed to ensure improved data security within the universities. It is recommended that the universities focus on malware control, business continuity and disaster recovery in their daily operations.

## REFERENCES

Blank, A., & Schiedel, L. (2003). *U.S. Patent Application No. 10/135,188*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Daya. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*.

Deloitte, L. L. P. (2011). Mobile telephony and taxation in Kenya. *Nairobi: Deloitte LLP*.

Deceulaer, D. (2016). Securing a school network and making it malware-free with limited resources: based on my experience in Mountains of the Moon University.

Eira, J. P., & Rodrigues, A. J. (2009). Analysis of WiMAX data rate performance. Lisbon: Instituto de Telecomunicaçõ̃es/Instituto Superior, Technical University of Lisbon.

Galliers, R. D., & Leidner, D. E. (Eds.). (2014). *Strategic information management: challenges and strategies in managing information systems*. Routledge.

Grama, J. (2014). Just in Time Research: Data Breaches in Higher Education. *EDUCAUSE*.

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*.

Kitheka, P. M. (2013). Information Security Management Systems in Public Universities in Kenya: A Gap Analysis between Common Practices and Industry Best Practices (Doctoral dissertation, University of Nairobi).

Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *Int. J. Comput. Sci. Secur. IJCSS*, *5*(1), 39.

Luambano, I., & Nawe, J. (2004). Internet use by students of the University of Dar es Salaam. *Library Hi Tech News*, *21*(10), 13-17.

Makori, E. (2013). Adoption of radio frequency identification technology in university libraries: A Kenyan perspective. *The Electronic Library*, *31*(2), 208-216.

Martins, A., Eloff, J. H. P., & Park, A. (2001). Measuring information security. In *Proceedings of Workshop on Information Security–System Rating and Ranking*.

Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.

Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.

Mingaine, L. (2013). Skill challenges in adoption and use of ICT in public secondary schools, Kenya. *International Journal of Humanities and Social Science*, *3*(13), 61-72.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.

Mullard, J. (207). Corrosion-induced cover cracking: new test data and predictive models. *ACI Structural Journal*, *108*(1), 71.

Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *Int. J. Comput. Sci. Secur. IJCSS*, *5*(1), 39.

Newswire, P. R. (2018). The Private LTE & 5G Network Ecosystem: 2018 - 2030 - Opportunities, Challenges, Strategies, Industry Verticals & Forecasts. *LON-REPORTBUYER*.

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2018). Understanding the Factors Affecting the Organizational Adoption of Big Data. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2016.1222891

Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.

Nweze, C. M. (2010). The use of ICT in Nigerian universities: A case study of Obafemi Awolowo University, Ile-Ife.

O'neil, P. (2014). *DATABASE: principles programming performance*. Morgan Kaufmann

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security*, *32*(2), 1.

Oguk, C., Karie, N., & Rabah, K. (2017). Network Security Management in Universities in Kenya. *Mara Research Journal of Computer Science & Security*, *2*(1), 48-60.

Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. *IEEE Security & Privacy*, *4*(8), 46-54.

Rabah, K. (2018). Convergence of AI, IoT, Big Data and Blockchain: A Review. *The Lake Institute Journal*.

Rabah, K., Research, M., & Nairobi, K. (2018). Enhancing Global Innovation Agenda www.thelakeinstitute.org The Lake Institute Convergence of AI, IoT, Big Data and Blockchain: A Review. In *The Lake Institute Journal*.

Sandvik, K. B. (2016). The humanitarian cyberspace: shrinking space or an expanding frontier?. *Third World Quarterly*, *37*(1), 17-32.

Makori, A. C., & Oenga, L. (2015). A survey of Information Security Incident. *Computers & Security*. https://doi.org/http://dx.doi.org/10.1016/j.cose.2014.11.006

Sandler, D., Derr, K., & Wallach, D. S. (2008). VoteBox: a tamper-evident, verifiable electronic voting system. *Proceedings of the 17th Conference on Security Symposium*.

Safer, A. (2012). A picture is worth a thousand words. *Marine Log*, 117-11.

Saleh, M. S., & Bakry, S. H. (2008). An overview of key IT risk management methods. *Saudi Computer Journal*, *6*(2), 61-70.

Selwyn, N. (2007). The use of computer technology in university teaching and learning: a critical perspective. Journal of computer assisted learning,23(2), 83-94.

Sekeres, M. A., & Bolwell, B. J. (2016). Will cancer patients be the next victims of the data privacy debate. *FoxNews. com. Accessed April*, *19*.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Stallings, W., & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice* (Vol. 6). London: Pearson.

Sridhar, S., & Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, *5*(2), 580-591.

Stallings, W., & Brown, L. (2008). Computer security. *Principles and Practice*. Stallings & Brown, (2008).

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). "Challenges of implementing e-learning in Kenya: A case of Kenyan public universities". *The International Review of Research in Open and Distributed Learning*, 16(1).

Tipton, H., & Krause, M. (2000). Information security management.

Tarus, D. K. (2015). Corporate social responsibility engagement in Kenya: Bottom line or rhetoric?. *Journal of African Business*, *16*(3), 289-304.

Tomlinson, G. (2012). *U.S. Patent No. 8,255,973*. Washington, DC: U.S. Patent and Trademark Office.