The Journal of Informatics, Vol. 3, Issue 1 (pages 51-67)
ISSN: 2714-1993
Received: July 2023, Published: December, 2023
https://doi.org/10.59645/tji.v3i1.127

****Original Research****

ASSESSMENT OF THE IMPACTS OF CYBER SECURITY ON STUDENT INFORMATION MANAGEMENT SYSTEMS: A CASE OF RUAHA CATHOLIC UNIVERSITY

Frowin R Kifaru
Faculty of Informatics
Institute of Accountancy Arusha

Karisha Daniel Kavuta
Faculty of Informatics
Institute of Accountancy Arusha

Adam Aloyce Semlambo
Faculty of Informatics
Institute of Accountancy Arusha

Abstract

The pervasive use of technology in education has posed a security challenge that could jeopardise student data and educational institutions' reputations, necessitating a thorough investigation. This study explores the impact of cybersecurity on Ruaha Catholic University's Student Information Management System. The research mainly employed a quantitative approach, with data collected through questionnaires administered to a diverse sample of 374 individuals, encompassing students and staff. In addition, a qualitative method was used to acquire data on the organisation's readiness to prevent cybersecurity threats from key informants, including system administrators and top management personnel. The Statistical Package for the Social Sciences (SPSS) software analysed the quantitative data using descriptive analysis. The study's results underscore the pressing need to develop effective cybersecurity mechanisms in the education sector, specifically focusing on enhancing the security of Ruaha Catholic University's Student Information Management System. The study recommends formulating and implementing robust cybersecurity strategies to safeguard student information, fortify system resilience, and bolster the institution's overall cybersecurity posture.

Keywords: *Cybersecurity, Student Information Management System, Ruaha Catholic University, Education technology, Data security*

1.0 INTRODUCTION

Educational intelligence has greatly improved the efficiency of the teaching process and the ability to manage and share educational resources, thereby continuously promoting education development (Kavuta & Nyamanga, 2018). However, in informatisation teaching and educational resource management, much information about education, teaching, and students' privacy has been involved and kept in Student Information Management systems (Kundy & Lyimo, 2019). Suppose the Student Information Management System stores and manages the information improperly. In that case, it will lead to the leakage of important information in the education and teaching process and the leakage of students' privacy.

This will have a huge negative impact on the education and teaching process and the protection of student privacy, and it will also pose a certain threat to the entire education and social security. Many learning institutions have adopted learning management systems in Tanzania. Using such technologies in higher learning institutions in Tanzania presents some benefits, including storing student details, professors' or schools’ personnel details, syllabi, timetables, and management details (Kavuta & Nyamanga, 2018). As learning management systems became popular in schools, many concerns arose, including school personnel concerns about data security and privacy. Cyber-attacks in higher education are still a major problem; the increasing number of attacks and their growing complexity have big implications for teaching and learning.

With the increasing reliance on technology in education, Student Information Management systems have become essential tools for efficient administration and decision-making processes (Kundy & Lyimo, 2019). Student Information Management Systems play a crucial role in educational institutions by managing and storing vast amounts of student data since it stores staff's and students' personal information, academic records, financial status, and research records. Despite the importance of the Student Information Management System in managing student’s information, it still faces some significant challenges and risks, particularly regarding cyber security. It faces an ever-growing threat landscape, with cyber attackers targeting their valuable data. Breaches in student information can lead to severe consequences, including identity theft, financial fraud, reputational damage, and legal liabilities.

Ruaha Catholic University faces these cyber security challenges as an esteemed educational institution. Protecting the privacy and security of student information is paramount to maintaining the trust and confidence of students, parents, faculty, and staff. Understanding the existing cyber security measures and potential vulnerabilities within the Student Information Management System infrastructure is crucial for safeguarding sensitive data (Lubua et al., 2022). Therefore, the problem addressed in this study is the lack of a comprehensive understanding of the specific cyber security risks, vulnerabilities, and measures needed to protect the student information stored in Ruaha Catholic University by conducting a detailed investigation into the cyber security of Student Information Management System, at Ruaha Catholic University (Mishra et al., 2022 & Kumar, 2018). Therefore, this study investigated the impacts of cyber-security on Student Information Management Systems, focusing on the Ruaha Catholic University.

2.0 OBJECTIVE OF THE STUDY

This study aimed to assess the impact of cyber security on the student management information system at Ruaha Catholic University.

3.0 LITERATURE REVIEW

This section discusses the literature associated with assessing cyber security in student management information systems at Ruaha Catholic University.

3.1 Theoretical Review

In examining the impact of cybersecurity on Student Information Management Systems at Ruaha Catholic University, this theoretical review section delves into three key theoretical frameworks that illuminate the multifaceted dimensions of cybersecurity and its implications for educational institutions. The Theory of Securitization, advanced by McGlinchey et al. (2021), offers a perspective beyond the conventional state-centric view of security, emphasising influential actors' intentional designation of security issues. Within the context of cybersecurity, Pickin (2020) highlights the securitisation of cyberspace, stressing the urgent need for government intervention in the face of systemic cybersecurity challenges.

Game Theory, a branch of applied mathematics (Patil et al., 2018), plays a pivotal role in understanding the dynamic decision-making processes in the cybersecurity domain, where one player's choices can influence others, shaping the overall outcome. This theory becomes particularly relevant in addressing the systemic nature of cybersecurity challenges and the imperative for government intervention. Lastly, the Theory of Multifactor Authentication, as Mohamed (2014) outlined, offers insights into enhancing cybersecurity measures through multiple independent authentication factors, addressing the need for robust security while simplifying user experience. These frameworks collectively inform the study's goal of analysing cybersecurity challenges at Ruaha Catholic University, focusing on their systemic nature and the proposal of effective mitigation strategies.

Incorporating these theoretical foundations, this research seeks to provide a comprehensive understanding of the cybersecurity challenges confronting Ruaha Catholic University's Student Information Management System, emphasising systemic dynamics. It aims to offer practical measures to mitigate associated risks and threats. Additional relevant in-text references may be integrated to enrich the theoretical underpinning of this study further.

3.2 Empirical Review on Cyber Security

Asgary (2016) analysed different risk management strategies involving information systems at York University, where inadequate ICT-related policies were a contributing factor. Lubua and Maharaj (2012) found that most African organisations operate without proper ICT-related policies, increasing various Information System security incidents. Lubua and Pretorius (2019) decided to develop a new cyber security policy framework for Tanzania organisations, though this framework was not specifically intended for learning institutions. Another study by Kundy and Lyimo (2019) exposes different cyber security threats to learning institutions in Tanzania and their relation to poor ICT-related policies.

Furthermore, the studies by Semlambo, Almasi, and Liechuka (2022a) and Semlambo, Leichuka and Almasi (2022b) showed how public higher learning institutions in Tanzania are struggling to adopt various ICT technologies in supporting teaching, learning and research with poor success. One contributing factor to such results is the poor formulation of ICT-related policies, including but not limited to Information Systems security policies. Also, the study by Semlambo, Sengati, and Angalia (2022c), through mixed methodology and a sample size of 157 participants, had the same conclusion that poor ICT-related policies contribute to the failure of adopting e-learning systems in Tanzania's public higher learning institutions. All these findings from different researchers, especially those in Tanzania, have the same conclusion: Public higher learning institutions in Tanzania have inadequate ICT-related policies to prevent security threats and vulnerabilities in different information systems. Since no just one principle governs the Information Systems security development or review process, as noted by Bandara (2014) and Aiafi (2017), This study focuses on reviewing various policies, methods, guidelines, and frameworks by different researchers endorsed by organisations specialised in Information Systems security to develop an Information System security policy framework suitable for all public higher learning institutions in Tanzania.

4.0 METHODOLOGY

This section elucidates the research methodology employed in this study, encompassing key facets of the research design, data collection, and ethical considerations.

4.1 Research Area

The research is in the Iringa Region, with Ruaha Catholic University (RUCU) as the primary research setting. RUCU was chosen as the research locale due to its substantial Student Information Management System and the availability of a diverse and information-rich student and staff population. RUCU is deemed an ideal source of pertinent data, aligning with the research objectives (Araka, 2016; Kothari, 2014).

4.2 Research Design and Approach

This study adopts qualitative and quantitative research design, facilitating a systematic and structured exploration of cybersecurity within Student Information Management Systems. The quantitative research approach incorporates descriptive statistics, including frequencies and percentages, to assess and summarise collected data (Araka, 2016; Kothari, 2014). On the other hand, the qualitative method was used to collect opinions through interviews with key informants, including 2 top management and 2 administrators. The key informants were interviewed to provide information on how the organisation is prepared to prevent the system from cyber security threats.

4.3 Population, Sampling Technique, and Sample Size

The research population encompasses 5 faculties at Ruaha Catholic University, comprising 5,650 individuals, 5,464 students and 186 academic and non-academic staff members. A systematic sampling technique was employed to manage the population's scale. The sample size was determined using Taro Yamani's formula, resulting in a sample of 374 participants, of which 362 are students and 12 are staff members (Wimmer & Dominick, 2000; Comry & Lee, 1992; Uakarn et al., 2021).

4.4 Data Collection and Analysis Methods

Data collection methods involve structured questionnaires featuring closed and open-ended questions and structured interviews. Primary data collected through the questionnaires was analysed using SPSS software version 27. The data underwent meticulous processing and cleaning and was presented using frequency tables and graphs (Araka, 2011; Jasrai, 2020).

4.5 Validity, Reliability, and Ethical Considerations

DOI: https://doi.org/10.59645/tji.v3i1.127

In line with ethical considerations, this research underscores the importance of protecting participants' privacy and confidentiality. Informed consent was diligently obtained from all participants—furthermore, ethical guidelines mandated that participants are not exposed to harm throughout the research process. The dignity of research participants was upheld, and their data were treated with the utmost confidentiality. The study was committed to ensuring the reliability and validity of research findings to enhance the credibility and accuracy of the data collected. These ethical considerations are fundamental to the research process and are based on the principles outlined by Bhandari (2022) and the research community's ethical standards.

5.0 RESULTS ND DISCUSSIONS

This section discusses the results of the findings on assessing the impacts of cyber security on student information management systems. The findings focus on cybersecurity awareness and practices, threats, measures and preparedness, backup, and training among staff and students of Ruaha Catholic University, as presented in subsequent subsections.

5.1 Cybersecurity Awareness and Practices

This sub-section delves into the findings related to respondents' awareness and behaviours concerning cybersecurity risks at Ruaha Catholic University's Student Information Management Systems. The research aims to shed light on the level of understanding among respondents and the measures taken to safeguard the institution's Student Information Management System against potential cybersecurity.

Table 1: Descriptive Statistics on Cyber Security Risks

ITEM	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**Mean**	**S.D**
There is strong anti-virus is currently installed in the computer room and is automatically enabled for automatic update	41 (11.4%)	42 (11.7%)	71 (19.8%)	127 (35.4%)	78 (21.7%)	**3.44**	**1.267**
You sometimes click/open advertisement links, during your Student Information Management System account	69 (19.2%)	88 (24.5%)	58 (16.2%)	86 (24.0%)	58 (16.2%)	**3.48**	**1.379**

You often backup your data to prevent data loss	45 (12.5%)	47 (13.1%)	52 (14.5%)	119 (33.1%)	96 (26.7%)	**3.48**	**1.343**
A phishing scam means that someone or a website tries to get personal information from you, for example, by accidentally signing into a Student Information Management System account or filling out a form on the website. Have you, or do you believe you have ever fallen victim to a phishing scam?	37 (10.3%)	89 (24.8%)	104 (29.0%)	84 (23.4%)	45 (12.5%)	**3.03**	**1.183**
The organisation's stored, transmitted, or accessed data are protected from unauthorised access.	62 (17.3%)	94 (26.2)	60 (16.7%)	83 (23.1%)	60 (16.7%)	**2.96**	**1.384**

Source: Research Data (2023)

The Mean and Standard Deviation (S.D) results about respondents' agreement with cybersecurity measures reveal that most respondents agree strongly regarding strong antivirus protection in the computer room and data backup practices. However, many respondents admit to sometimes clicking on potentially risky advertisement links and falling victim to phishing scams (McGlinchey et al., 2021). These findings align with the Theory of Securitization, indicating a securitisation of cybersecurity within the university community. Nevertheless, there is a need for heightened awareness regarding online risks and safe behaviours, reinforcing the importance of continuous security training and awareness campaigns (Hamid et al., 2018). This analysis underscores the securitisation of cybersecurity and the ongoing efforts required to enhance information protection within the academic environment.

Overall, the findings in this section reveal a mixed landscape of cybersecurity awareness and practices at Ruaha Catholic University. While there is a commendable recognition of the importance of antivirus protection and data backup (McGlinchey et al., 2021), the prevalence of clicking on potentially risky advertisement links and falling victim to phishing attacks calls for more rigorous cybersecurity education and training. The results emphasise the need for continuous efforts to strengthen information protection in the academic setting, aligning with the existing literature's emphasis on enhancing cybersecurity awareness and practices (Hamid et al., 2018).

5.2 Cybersecurity Incidents

This sub-section provides insights into respondents' awareness and practices concerning cybersecurity incidents at Ruaha Catholic University's Student Information Management Systems. The aim is to shed light on their preparedness and knowledge regarding potential cybersecurity threats.

Table 2: Descriptive Statistics on Cybersecurity Incidents

ITEM	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	S.D
There is stealing personal information - the absence of privacy and occurrence of unauthorised access that causes the loss of data confidentiality, integrity, and availability at the Student Information Management System,	88 (24.5%)	72 (20.1%)	63 (17.5%)	81 (22.6%)	55 (15.3%)	2.84	1.414
There is the existence of data modifications in the Student Information Management System,	65 18.1%	99 27.6%	50 13.9%	84 23.4%	61 17.0%	2.94	1.384
There is the existence of viruses/Malicious that tend to damage an institution's system and network infrastructures	86 (24.0%)	87 (24.2%)	58 (16.2%)	79 (22.0%)	49 (13.0%)	2.77	1.386
There is an incident of unauthorised access to my Student Information Management System, account	82 (22.8%)	100 (27.9%)	65 (18.1%)	64 (17.8%)	48 (13.4%)	2.71	1.351
There is system downtime or operational failures of Student Information Management System in Institutions due to cyber attacks	63 (17.5%)	70 (19.5%)	74 (20.6%)	96 (26.7%)	56 (15.6%)	3.03	1.339

Source: Research Data (2023)

Table 2 presents Mean and Standard Deviation (S.D) findings regarding respondents' agreement with various cybersecurity incidents. It reflects a nuanced landscape of awareness and concerns within the university community. For example, respondents exhibit significant concerns about stealing personal information, data modifications, and unauthorised access, with varying levels of agreement and disagreement. However, there is less consensus regarding viruses and malicious software, suggesting a need for more comprehensive education on these potential threats. The concerns about unauthorised access and system downtime emphasise the importance of safeguarding data and system availability. These findings resonate with the Theory of Securitization, which posits that issues become security concerns when labelled as "dangerous" or "threatening" by influential actors (McGlinchey et al., 2021). Overall, the results underscore the significance of continuous efforts to strengthen information protection and cybersecurity awareness within the academic environment, aligning with existing literature's emphasis on enhancing cybersecurity awareness and practices (Hamid et al., 2018).

5.3 Cybersecurity Measures

In this sub-section, the perceptions and opinions of respondents at Ruaha Catholic University regarding the cybersecurity measures in place are examined. Understanding how the academic community perceives the institution's management efforts and practices in safeguarding sensitive information.

Table 3 Descriptive Statistics Cyber security measures

ITEM	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**Mean**	**S.D**
The institution regularly tends to improve or review internal controls to prevent malicious Student Information Management Systems,	19 (5.3%)	29 (8.1%)	91 (25.3%)	144 (40.1%	76 (21.2%)	3.64	1.066
Data that is stored, transmitted, or accessed by the organisation is protected from unauthorised access	26 (7.2%)	40 (11.1%)	78 (21.7%)	133 (37.0%)	82 \922.8)	3.57	1.167
There is the availability of ICT facilities and strong technology, which helps in minimising data altering and interception in the institute ISMS	17 (4.7%)	22 (6.1%)	96 (26.7%)	134 (37.3%)	90 (25.1%)	3.72	1.055
The institute has developed written policies and procedures to manage and control risks in ISMS	28 (7.8%)	61 (17.0%)	87 (24.2%)	109 (30.4%)	74 (20.6%)	3.39	1.209
You were once trained to safeguard the Student Information Management System, access information, and prevent, detect, and respond to cyber threats and attacks	30 (8.4%)	60 (16.7%)	68 (18.9%)	116 (32.3%)	85 (23.7%)	3.46	1.250

Source: Research Data (2023)

Table 3 presents Mean and Standard Deviation (S.D) findings regarding respondents' agreement with various cybersecurity measures. It reveals a nuanced perspective within the academic community: The findings indicate that respondents are confident in the institution's cybersecurity measures. The results align with the emphasis in existing literature on the need for continuous improvement in cybersecurity policies and practices, particularly in educational institutions (Hamid et al., 2018).

The response variability highlights the importance of addressing training gaps and enhancing internal controls to ensure a robust cybersecurity posture. Additionally, these findings align with the Theory of Securitization, which suggests that issues become security concerns when labelled as "dangerous" or "threatening" by influential actors (McGlinchey et al., 2021). The strong agreement with specific cybersecurity measures reflects the securitisation of cybersecurity within the university community, where certain actions and practices are recognised as essential for information protection. To further strengthen the institution's cybersecurity posture and protect sensitive information from potential threats, addressing training needs, standardising policies and procedures for risk management, and continuously reviewing and enhancing internal controls are essential steps to consider.

5.4. Cybersecurity Threats and Preparedness

This sub-section focuses on the responses to cybersecurity threats and preparedness at Ruaha Catholic University, which is essential for assessing the institution's overall security posture. The interview results with the key informants revealed that there had been no serious operation failure caused by malware attacks, no existence of unauthorised access, and no interception during data transmission. Additionally, the informants revealed through interviews that the university has protected their system and users by preventing them from cybersecurity threats. The organisation has a long-term strategy, sufficient ICT staff and facilities, and robust technology, which help minimise data alteration and interception. The physical environment is secured by installing various detectors for potential cybersecurity events. Lastly, the findings reveal that regular training is conducted within an organisation to safeguard the Student Information Management System, access information, and prevent, detect, and respond to cyber threats and attacks.

Based on these findings, it is revealed that there is a high level of confidence in the institution's cybersecurity resilience. The responses align with the theory of securitization, reflecting a proactive approach to securing the university's information systems (McGlinchey et al., 2021). Various aspects of cybersecurity readiness signify the securitisation of these issues, emphasising their importance within the institution's framework. To maintain and enhance cybersecurity preparedness, Ruaha Catholic University should continue monitoring potential threats, updating policies and procedures, and ensuring regular training for all staff and students. Sharing best practices with other institutions can contribute to a culture of cybersecurity awareness and collaboration within the academic community.

5.5. Data Backup Practices among Responders

This subsection explores the respondents' data backup practices and attitudes towards preventing data loss. Table 4 summarises the responses and provides insights into the participants' backup habits.

Table 4: Backup Practise among Respondents

	Agree	Disagree	Neutral	Strongly agree	Strongly Disagree	Total
Staff	3	1	2	2	2	10
Student	116	46	50	94	43	349
Total	119	47	52	96	45	359

Source: Research Data (2023)

The responses in Table 4 reveal the attitudes and practices of participants regarding data backup. Notably, many students agree (116) and strongly agree (94) that they often back up their data to prevent data loss, indicating a proactive approach to safeguarding their information. However, some individuals disagree (47) or strongly disagree (43) with the practice of data backup, suggesting that some respondents might not prioritise this essential aspect of data security.

In alignment with existing literature, the significance of data backup in preventing data loss is well-established. These findings underline the importance of fostering awareness and promoting the habit of regular data backup among the university community to mitigate the risk of data loss.
Applying these results to the Theory of Securitization, it becomes evident that data backup is a securitised issue among respondents. The strong agreement and disagreement responses highlight this matter's polarised nature, emphasising the need for targeted awareness campaigns and training. The institution should consider implementing educational initiatives and resources that encourage and enable all participants to adopt data backup practices. The institution can further enhance its overall cybersecurity posture and data resilience by addressing the disparities in responses and promoting a collective commitment to data security.

5.7 Cybersecurity Training Among Responders

This subsection delves into the respondents' experiences with cybersecurity training, specifically regarding safeguarding the Student Information Management System, accessing information, and preventing, detecting, and responding to cyber threats and attacks. Table 5 summarises the responses and provides insights into the participants' training experiences.

Table 5: Cybersecurity Training Among Respondents.

	Agree	**Disagree**	**Neutral**	**Strongly agree**	**Strongly Disagree**	**Total**
Staff	2	3	2	3	0	10
Student	114	57	66	82	30	349
Total	116	60	68	85	30	359

Source: Research Data (2023)

The responses in Table 5 shed light on the participants' experiences with cybersecurity training. Notably, many students agree (114) and strongly agree (82) that they have received training to safeguard the Student Information Management System, access information, and prevent, detect, and respond to cyber threats and attacks. This indicates that many students have been exposed to cybersecurity training. Conversely, some individuals, staff and students, reported disagreeing or strongly disagreeing with receiving such training. This highlights a gap in training and awareness that should be addressed to ensure all university community members are well-equipped to deal with cybersecurity challenges.

In alignment with existing literature, the importance of cybersecurity training in preventing and mitigating cyber threats is well-documented. These findings underscore the significance of offering comprehensive training programs to enhance staff and students' cybersecurity knowledge and skills. Applying these results to the Theory of Securitization, it becomes evident that cybersecurity training is a securitised issue among respondents. The disparity in responses emphasises the need for a more uniform and inclusive approach to training and awareness efforts.

The institution should prioritise and expand its cybersecurity training initiatives to ensure that all staff and students receive the necessary education and guidance to protect the Student Information Management System, access information securely, and respond effectively to cyber threats. This approach will contribute to a more resilient and secure cybersecurity environment within the university.

6.0 CONCLUSION AND RECOMMENDATION

This study sheds light on the cybersecurity landscape at Ruaha Catholic University by examining the perceptions, attitudes, and practices of both staff and students. The findings reveal a high awareness and commitment to cybersecurity measures, with strong agreement on critical aspects such as antivirus protection and data security. However, disparities exist in data backup practices and cybersecurity training, emphasising the need for targeted awareness campaigns and training initiatives to bridge these gaps. The Theory of Securitization is evident in the securitisation of cybersecurity within the university community, where specific actions and practices are recognised as essential for information protection. To enhance the institution's cybersecurity posture, it is crucial to address these disparities, prioritise training, and implement a holistic approach to cybersecurity, fostering awareness and collaboration within the academic community.

Based on the findings of this study, several recommendations are put forth to strengthen the cybersecurity posture of Ruaha Catholic University. Firstly, the institution should develop and implement comprehensive ICT policies and procedures to ensure a standardised and proactive approach to risk management. Secondly, there is a pressing need to expand and enhance cybersecurity training programs for staff and students to ensure they are well-equipped to handle emerging cyber threats effectively. Furthermore, the university should prioritise raising awareness about the importance of regular data backup practices among its academic community. Lastly, continuous physical environment monitoring for potential cybersecurity events should be emphasised. By taking these steps, Ruaha Catholic University can foster a culture of cybersecurity awareness and collaboration, ensuring the protection of its information systems in an ever-evolving digital landscape.

REFERENCES

Alexei, A. (2021) 'Cyber Security Threat Analysis in Higher Education Institutions As A Result of Distance Learning', International Journal of Scientific and Technology Research, 128-129.

Araka, J. (2016) Fundamentals of Communication Research in Africa: A Contemporary View, University of Dar es Salaam Library Journal, 14(1), 134-136.

Arina, A. (2021) 'Cyber security strategies for Higher Education. Journal of Engineering Science', Journal of Engineering Science Fascicle, 74 – 92.

Bhandari, P. (2022) Ethical Considerations in Research | Types & Examples. Available at:

https://www.scribbr.com/methodology/research-ethics/ [Accessed 9 February 2023].

Bresnick, P. (2021) 4 Reasons Cyber Criminals Are Targeting Higher Education: Part 1. Available at: https://www.fierceeducation.com/best-practices/4-reasons-cyber-criminals-are-targeting-higher-education-part-1 [Accessed 2 January 2023].

Campbell, S. (2020) Cybersecurity in Higher Education: Problems and Solutions. Available at: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education [Accessed 24 January 2023].

Chandarman, R. & Niekerk, B. (2017) 'Students' cybersecurity awareness at a private tertiary educational institution', The African Journal of Information and Communication, 138-144.

Chin, K. (2022) How Colleges & Universities Can Prevent Ransomware Attacks. Available at: https://www.upguard.com/blog/how-colleges-and-universities-can-prevent-ransomware-attacks (Accessed 2 January 2023).

Chizanga, M. K., Angola, J. & Rodrigues, A. (2022) 'Factors Affecting Cyber Security Awareness'. International Research Journal of Innovations in Engineering and Technology (IRJIET), 54-55.

Cisco (2020) Network Readiness Index 2021, Venezuela: Portulans Institute. Available at: https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/country/TZA (Accessed 23 January 2023).

Cyber Management (2022) Cybersecurity for Higher Education Institutes: Impact & Solutions. A vailable at: https://www.cm-alliance.com/cybersecurity-blog/cybersecurity-for-higher-education-institutes-impact-solutions (Accessed 2 January 2023).

Eker. C H., Zhuang, J. & Upadhyaya, S. (2016) ''Deception-Based Game Theoretical Approach to Mitigate DoS Attacks'. Springer International Publishing, 1 (10), 20-22.

Ekran, S. (2020) Cybersecurity Compliance in the Education Industry: How to Protect Students' Data. Available at: https://www.ekransystem.com/en/blog/cybersecurity-in-educational-institutions (Accessed 10 December 2022).

ESDC (2018) Education sector development plan (2016/17 – 2020/21), Dar es Salaam: MEST. Available at: https://www.globalpartnership.org/sites/default/files/2019-04-gpe-tanzaniaesp.pdf

Fouad, N, (2021) Securing higher education against cyber threats: from an institutional risk to a national policy challenge, Journal of Cyber Policy, 6(2), 137-154, DOI: 10.1080/23738871.2021.1973526

Gupi, M. (2022) 'Human factors in Cybersecurity: Risks and impacts'. Institute for Electronic Business, pp. 57-58.

Hunt, T. (2016) Cyber Security Awareness in Higher Education. *Central Washington University*, 1-14.

IBM & Ponemon Institute (2019) Cost of a Data Breach Report. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report (Accessed 7 2 2023).

Jisc (2020). 'The Impact of Cyber Security Incidents on the UK's Further and Higher Education and Research Sectors. 12-18

Kaspersky (2018). Top 5 Most Notorious Cyberattacks. [Online] Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report [Accessed 25 January 2023].

Kaspersky, 2022. Resource Center. [Online] Available at: https://www.kaspersky.com/resource-center/definitions/data-breach

Kavuta, K and Nyamanga, S. (2018) The factors affecting the implementation of students' records management system to higher learning institutions in Tanzania: A case of the institute of Accountancy Arusha, *International Journal of Scientific & Technology Research, 7(2), 150-156.*

Kothari, C. P. (2014) Research Methodology: Methods and Techniques. 3 Ed. New Delhi: New Age International (P) Limited.

Kumar, D. K. (2018) 'Impact of modern technology in'. Academia, Volume 381.164, pp. 33-34.

Kundy, E. D. & Lyimo, B. J. (2019) "Cyber security threats in higher learning Institutions in Tanzania', A case of the University of Arusha and Tumaini University Makumira. Olva Academy –School of Researchers, 2(3).

Lakshmanan, A. (2019) 'Literature review on Cyber Crimes and its Prevention Mechanisms'. researchgate, Volume 6, p. 1.

Lymo, B. J. (2019) 'Assess the cyber security threats in higher learning Institutions in Tanzania, A case of the University of Arusha and Tumaini University Makumira. Olva Academy School of Researcher, pp. 4-5.

Maraj, A., Sutherland, C. & Butler, W. (2021) The Challenges to Cybersecurity Education in Developing Countries. Academic Conferences International Limited, p. 260.

Matandiko, K. (2017) ‘Wahalifu wa kimtandao wavamia tovuti ya Chuo Kikuu Huria’. Daily Nation, 24 October, 2017.

McGlinchey, S., Waters, R. & Scheinpflug, C. (2021) ‘Securitisation Theory. The LibreTexts Libraries', p. 14.

Merrigan, G. & Huston, C. L. (2004) Communication research methods. Belmont. CA: Thomson Wadsworth, pp. 10-15.

Mohamed, S. T. (2014) 'Security of Multifactor Authentication Model to Improve Authentication Systems'. IISTE, 4(6), pp. 81-82.

Naden, C. (2019). Stronger data protection with updated guidelines on assessing information security controls. Available at: https://www.iso.org/news/ref2367.html (Accessed: 11 February 2023).

Patil, A. P., Bharath, S. & Annigeri, M. N. (2018) 'Applications of Game Theory for Cyber Security System'. A Survey. Ripublication, 13(17), pp. 12987-12988.

Pickin, M. (2020) 'What is the securitization of cyberspace? Is it a problem?'. Academia, pp. 8-9.

Semlambo, A. A., Mfoi, D. M. & Sangula, Y. (2022) 'Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA)'. Journal of Computer and Communications, pp. 26-43.

Lubua, E. W., Semlambo, A. A.,& Mkude, C. G. (2022) ‘Factors affecting the security of Information Systems in Africa. University of Dar es Salaam Library Journal, Vol 17, No 2 (2022), pp 94-114.

Tassaddiq, A. & Alharbi, T. (2021) 'Assessment of Cybersecurity Awareness among Students of

Majmaah University'. Big data and cognitive computers, pp. 8-15.

Uakarn, C., Chaokromthong, K. & Sintao, N. (2021). Sample Size Estimation using Yamane Cochran and Krejcie. Apheit International Journal, pp. 78-79.