ABSTRACT

Authentication, authorization, encryption intrusion detection and prevention are the major indicator for LAN security which together insures confidentiality, integrity and availability of data/information for the users. Many studies had been conducted in different parts in the world on the factors influencing LAN security such as Network design, firewall configuration, physical protection and separation by physical, logical, and encryption methods for data protection. Regardless of the above factors the problem were still exist. This research uses factors such as security policy, security awareness, encryption technology, authentication and authorization, penetration test and vulnerability assessment to fill the gap, by putting into consideration the purpose of the study which was primarily to explore the factors that determining the levels of security of LAN. This study was carried out at Stefano Moshi Memorial University College (SMMUCo) and Mweka College of Wildlife Management in Moshi municipal by using self-administered questionnaire to 60 respondents of which were only staffs. The overall results of research showed that the institutions currently are adapting normal techniques to secure their LAN of which makes them to be at risks due to the tremendous advancement of technology. In respect to the study conducted policy implication is very significant this is due to the high volume of the network users which increases the chance of getting in for intruders. Some of the institution surveyed has security policy which is well documented but lacks practical implementation for its effectiveness. Also the study revealed that there is gap between user's knowledge on security features and its applicability like turning on their firewall, encrypting their data and periodic change of their password it is a challenge so setting up rules and regulations which enforcing them to adopt is very important. Some of the HLIs had wireless network which provide connections to various users implementing security policy will help to reduce some risks associated with user awareness on security issues especially on maintaining confidentiality, integrity and availability of their information Challenges they face involving existing practices, boosting awareness and tightening security policies. This signifies that implemented techniques are not much satisfies data protection; hence it can be difficult to fight against hackers.