ABSTRACT

The use of information and communication technology has been providing the competitive edge for universities globally while Kenyan universities are not an exception. This has in turn made the universities targets of cyber-attacks and hence exposure to unprecedented security risks. The universities need to implement information security best practices and standards in their technological environments to remain secure and operational. The research sought to investigate the information security practices adopted in Kenyan public universities to protect themselves. Descriptive survey method was employed while the study was based on Operationally Critical Threats, Assets and Vulnerability Evaluation (OCTAVE) framework and other industry security best practices. The study targeted the 31 chartered public universities, whichwere clustered based on their year of establishment. Simple random and purposive sampling methods were utilized to select two target universities per cluster and determine respondents respectively. The study had a response rate of 61%. Analysis of data was done via descriptive statistics while presentation of results was done using tables and Likert scale. The study revealed that universities had implemented information security policies, with 47.6% of respondents somewhat agreeing to that. Funding for security was provided 57.6% somewhat agreeing, though the funding was deemed low by 51% of respondents. Training for security staff was deemed somewhat available (44%) thus below par, while involvement of university management on policies development was at 48% though university management participation in policies review was below average. 38% of respondents somewhat agreed that policies governing use of mobile devices existed. Frequency of user awareness and training was below the average, while48% of respondents somewhat agreed that universities usually share their intelligence reports on threats and responses with other government agencies. 49% of respondents were somewhat in agreement universities had put in place incidence response plans. Application of updates and improvements was below average, though evaluation of effectiveness of controls was average. To remain protected universities management should cause a review of their employed information security practices and address identified gaps through instigation of essential remedial actions.