ABSTRACT

Modern days have seen an uncontrolled increase in cybercrime, targeting both developing and developed countries and more so the telecommunications sectors. Unfortunately, Cybersecurity frameworks, used by organizations to counter cybercrime, have failed in one way or another to ensure responsive and substantive security in developing countries. There is, therefore, a need for cost-effective and responsive cybercrime framework in the telecommunication sector in developing country. It based on this premise that the present study was carried out. This research sough to assess a cybercrime framework applicable to Kenyan telecommunications sector. The objectives of the research was to examine the cybercrime in telecommunications industry in Kenya; to establish the cybercrime frameworks currently used by telecommunications companies in Kenya and to propose a cybercrime framework applicable to Kenyan situation. The study used descriptive research design in soliciting information in the research of to assess the factors contributing to Cybersecurity Framework in Kenya. The target population was the 121 Information Technology experts in the telecommunications industry in Kenya. The study obtained a sample size of 92 respondents using the Slovin‟s formula The study adopted proportionate stratified random sampling to select the respondents form each company. Data was collected using a structured questionnaire administered using the drop and pick method. The research tool (questionnaire) was first tested for reliability and validity before administration. The study analyzed the data using descriptive analysis to produce descriptive statistics. Thereafter inferential analysis was carried out to establish a study model. The study concludes that personal data protection demands very highly contributes to development of the Cybersecurity framework in Kenyan telecommunications companies; computer use control highly influences the development and adoption of Cybersecurity framework in Kenyan telecommunications companies; content exposure control highly contributes to Cybersecurity framework development in Kenyan telecommunications companies; and data copyright structures highly influences the Cybersecurity framework in Kenyan telecommunications companies. The study reveals that at 0.05 (5%) level of significance, personal data protection demands, computer use control, content exposure control, and data copyright structures are predictors of the Cybersecurity framework in Kenyan telecommunications companies. Each of computer use control and content exposure control has a significant positive relationship with Cybersecurity framework in Kenyan telecommunications companies while personal data protection demands has a moderate significant relationship and data copyright structures has negative insignificant relationship. It was established that 60.000% of change in Cybersecurity framework in Kenyan telecommunications companies is explained by personal data protection demands, computer use control, content exposure control, and data copyright structures. The study recommends that the Kenyan telecommunications companies should; enhance their personal data protection structures to fully protect their clients‟ data; unilaterally review the computer use controls for the adoption of Cybersecurity framework; come together to creation and development of content exposure control based Cybersecurity framework and advocate for strict law as on copyright related offences.