ABSTRACT

This research Dissertation has evaluated post-cyber disaster recovery preparedness in higher learning institutions in Arusha. It recognizes the potential risks and consequences posed by cyber-attacks, including data breaches and system disruptions. The study has assessed the effectiveness of existing cyber disaster recovery plans and identified opportunities for improvement to enhance the resilience of educational institutions against cyber threats. The research has employed a mixed-methods approach, including both qualitative and quantitative data collection techniques. Interviews and questionnaires were conducted with key stakeholders, including IT personnel and administrators totaling a sample of twenty-six (26) participants, to gather insights on the current state of cyber disaster recovery preparedness. this study has highlighted the varying levels of preparedness among higher learning institutions when facing cyberattacks. While these institutions undertake preparations such as data backups and training, it's essential to acknowledge their general absence of a formal cybersecurity framework. Higher learning institutions must develop formal recovery plans for cyber disasters and it is best to adopt an international standard that will help the higher learning institutions to transition smoothly from disruption back to full operation example of such a standard is ISO 22301:2019 business continuity framework.