Abstract:

The primary focus of the study was to find out the extent of management awareness of the potential risks facing computer based financial information systems and the preventive measures undertaken. The reviewed literature indicated increased use of computers in the processing of data in the banking industry. It also indicated the increasing magnitude of computer crime in both the number of incidences and losses incurred. This trend is expected to continue. Consequently, management must design effective control measures to contain these threats. The literature emphasized that security considerations are of paramount importance in computerised financial information systems. The literature also indicated user ignorance of the nature of special kinds of risks facing computerised systems and consequently of the appropriate measures that should be taken to manage and control such risks. The population of interest for this study comprised the 24 commercial banks and 54 financial institutions registered under the Banking Act and operating in Kenya as at 30th June 1988. A census study covering all the 78 institutions was carried out. The findings of the study suggested that most of the risks perceived by management were of a physical nature: Fire, power surges and floods. The other more elusive and dangerous risks whose materialization would lead to unauthorised interruption, corruption, destruction, removal or disclosure of data and computer resources were not given sufficient consideration. The observations indicated apparent ignorance of the authorized user or the company's own employees as the major threat facing computerised systems. The findings of the study also suggested that the measures undertaken by management to contain the computer risks placed emphasis on the traditional approach access control, fire guards, power stabilizers, etc. Operator/clerical errors, machine (hardware) failure, power failure and magnetic media failure were the most commonly experienced problems. Huge losses were also reported due to frauds and spillage damage. From the study it is apparent that security awareness and control measures were weak. Given the varied nature of actual problems experienced, the study suggested that the measures typical in the traditional approach left unattended the more serious and frequent security problems. An appreciable proportion of the measures undertaken appeared to be either ineffective or very risky. This situation appeared to increase the potential for error, fraud, sabotage and unauthorised access to confidential information on many computer systems. In conclusion, some suggestions for strengthening security of computer based financial information systems were made. These included increasing the management awareness by attending seminars on computer security organised by auditors, dealers, manufacturers and suppliers of computer hardware and software. Employee awareness could also be increased through continuous staff education on security considerations.