ABSTRACT

Securing the organisational data and information system is one of the main concerns in any organisation in the present world. Value of the military information cannot compare with any other organisational information. Lost, damage or change of such information may costly even for the national security. Sri Lankan military forces also recognise cyber threat as a non-traditional threat to its operations as well to the national security. Defence Services Command and Staff College (DSCSC) adopt some of the cyber security procedures to mitigate potential cyber threat. This research was focussed on identify the vulnerabilities of DSCSC for the potential cyber threats and propose better solution to mitigate such vulnerabilities. The study was mainly concentrated towards physical security vulnerabilities and user vulnerabilities aspects. This study deeply analysed the existing computer network, information systems and user status of the DSCSC information system. The study was conducted in qualitative method and participatory observation, formal and informal interviews are the primary source of data in this research. The data gathered through field interviews, audio recordings and transcripts. Further the researcher used internationally recognised tools and methods to identify the vulnerabilities of DSCSC computer network. Most of the tools were developed according the ISO 27001 standards. These tools were used to measure the threat level of the each selected element in the DSCSC information system. The tools developed in this study could be used to test the threat level of any of similar organisation. After the in-depth analysis, the feasible solutions were proposed to prevent and mitigate the existing cyber security threat to DSCSC.