Abstract

This study was prompted by the recent connectivity of Arusha town to the fibre cable in Dar-es-salaam namely the Seacom and Essay fibre cable in May, 2010. This enhanced connectivity significantly improved the downloads and uploads speed of traffic to and from Arusha consequently greatly improving the users experience of Internet related services now traveling at lightening speeds. This opened up the possibility of effectively using internet related business services like online tax processing, banking and educational services that were previously to slow too run on satellite (VSAT) or dial-up links and triggered a need or awareness for businesses in Arusha to start using as well incorporating more Internet related business services in their daily operations to effectively compete.

Unfortunately with this improved connectivity and subsequent increase in business opportunities could also have generated additional interest in the region by Cyber (Internet related) crime perpetuators as well as amplified exposure to Cyber threats as connecting to machines in Arusha from anywhere in the world had become faster and easier. The consequences of these threats/attacks are well-known: violation of privacy, theft of information, the potential for a devastating large scale network failure, service interruption, or the total unavailability of service. This change therefore passes a question to small and medium enterprises/businesses (SME's) in Arusha; *as to whether they are adequately prepared to meet this new challenge and if not what could these SME's do about it?*

This research therefore set out to assess the efforts of SME's in Arusha in the realm of cyber security. Attention was directed to SME's because SMEs are the engine of the national economy and account for over 95% of organizations and 60-70% of employment (OECD, 1997). When approaching this problem, the researcher noted that though in the past; traditional definitions of cyber security have been to design strong cryptography into information security systems. Only protecting confidential information as a motivation for cyber security may not be entirely appropriate for SME's.

More so there had been increasing interest in other sectors of security, namely geo-political, economic and human previously considered by many as non-traditional