ABSTRACT

The effectiveness of the cyberspace protection for the national Critical Information Infrastructure (CII) depends on a dynamically and reliably established cyberspace situational awareness framework. The current attribution based cyberspace protection models and frameworks are characterised by over dominance of government agencies and laws, over-reliance on technology and lack of trust, transparency and goodwill leading to weak protection of critical information infrastructure. The general objective of this study was to develop an enhanced situational-aware cyberspace protection framework for CII. The specific objectives of the research were: To assess the existing situational-aware frameworks for cyberspace protection for Cll; to evaluate the influence of the maturity of cyberspace regulatory frameworks on situational-aware cyberspace protection for Cll; to determine the influence of crowdsourcing on situational-aware cyberspace protection for Cll; to determine the influence of cognitive agility of cyber protection operators on situational-aware cyberspace protection for Cll, and to develop an enhanced situational-aware cyberspace protection framework for CI!. The study adopted a descriptive research design using questionnaires. Data was then analyzed using mean, standard deviation, frequency distributions, Pearson's correlations and Linear Regression Analysis using the Statistical Package for Social Sciences (SPSS) software, then presented in tables and figures. The study established that the availability of effective regulatory bodies to champion and govern the cyberspace has a positive impact towards the realisation of the desired cyberspace protection objectives. Crowdsourcing was found to positively influence situational-aware cyberspace protection. This implies that the various previous crowdsourcing models and successes can be considered to improve the cyberspace protection of CIJ. The study revealed that there was a statistically significant moderate and positive association /relationship between cognitive agility and situational-aware. This implies that the cyberspace protection is as strong or as weak as the cyberspace protection operators. The study concluded that a human-factored security endeavour is required that can improve the capabilities of the operational technology human constituents, so that they can appropriately recognise and respond to cyber intrusion events within the Cll environment. Amidst evolving security trends that places human industrial actors as prime vectors of CII cyber-attacks, human-factored security efforts are required to manage and control the menace of prevailing attacks. It's invaluable considering that cyber security knowledge and skills capabilities of the Cll workforce (people) is crucial and strategic towards building a more effective and cybersecurity-compliant workforce.