Lecture Notes in Networks and Systems

Conceptual mapping of the cybersecurity culture to human factor domain framework

Emilia N. Mwim[1], Jabu Mtsweni[2], Bester Chimbo[1]

[1]Department of Information Systems, School of Computing, College of Science Engineering and Technology, Unisa. Florida, South Africa

[2]Head of Information and Cyber security Centre, CSIR, Pretoria, South Africa

https://doi.org/10.1007/978-3-031-28073-3_49

Abstract

Human related vulnerability challenges continue to increase as organisations intensify their use of interconnected technologies for operations particularly due to the emergence of COVID-19 pandemic. Notwithstanding the challenge of a human problem on cybersecurity, existing cybersecurity measures predominately focused on technological solutions which on their own have proven to be insufficient. To ensure all-inclusive cybersecurity solution, efforts are shifting to accommodate human angle which complements technological efforts towards eradicating cybersecurity challenges hence the move to cybersecurity culture (CSC). The importance of the human-related factor on the security of information and IT system has been emphasised by various research leading to the development of Human Factor Diamond (HFD) framework. This paper at the conceptual level mapped the articulated list of identified CSC factors to the HFD framework to determine the CSC factors that are associated with the different domains of human factor framework. The mapping depicts that each domain of human factor framework has CSC factors associated to it. Management appeared as the domain with the predominate number of factors, followed by responsibility, environment and preparedness respectively.