Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan

Authors : Pema Choejey, David Murray, Chun Che Fung

Abstract : Bhutan is becoming increasingly dependent on Information and Communications Technologies (ICTs), especially the Internet for performing the daily activities of governments, businesses, and individuals. Consequently, information systems and networks are becoming more exposed and vulnerable to cybersecurity threats. This paper highlights the findings of the survey study carried out to understand the perceptions of cybersecurity implementation among government organizations in Bhutan. About 280 ICT personnel were surveyed about the effectiveness of cybersecurity implementation in their organizations. A questionnaire based on a 5 point Likert scale was used to assess the perceptions of respondents. The questions were asked on cybersecurity practices such as cybersecurity policies, awareness and training, and risk management. The survey results show that less than 50% of respondents believe that the cybersecurity implementation is effective: cybersecurity policy (40%), risk management (23%), training and awareness (28%), system development life cycle (34%); incident management (26%), and communications and operational management (40%). The findings suggest that many of the cybersecurity practices are inadequately implemented and therefore, there exist a gap in achieving a required cybersecurity posture. This study recommends government organizations to establish a comprehensive cybersecurity program with emphasis on cybersecurity policy, risk management, and awareness and training. In addition, the research study has practical implications to both government and private organizations for implementing and managing cybersecurity.