Cybersecurity Challenges and Practices: A Case Study of Bhutan

Pema Choejey, Murdoch University, Perth, 2018

Abstract

Bhutan is an emerging country with transitioning economy with a vision to become an ICT knowledge-based information society. Many government organizations, businesses and individuals are adopting the Internet for day to day operations and activities. With increasing dependency on information systems, networks, and the Internet; securing and protecting Bhutan’s cyberspace from malicious attackers and cyber criminals is a serious concern.

Few scholarly studies related to cybersecurity have been conducted in developing countries. No scholarly and empirical research has been conducted in Bhutan to understand how the government is addressing and managing cybersecurity. This has resulted in a critical knowledge gap that must be addressed urgently through empirical research to guide government policy makers, security professionals and practitioners to develop and implement cybersecurity program. This thesis investigates the development and implementation of cybersecurity policies and practices in government organizations in Bhutan.

A sequential mixed methods research design was employed to collect primary data on cybersecurity risks, effectiveness of cybersecurity policies and practices, and perceptions of cybersecurity in government organizations. The research also used secondary data sources such as government reports, print and social media, to validate the results of the research study.

The findings suggest that government organizations in Bhutan are vulnerable to cybersecurity risks, such as malware and hacking, and that they lack adequate knowledge and awareness of cybersecurity, cybersecurity policies and procedures, technical controls, and incident response capabilities. Furthermore, the evidence suggests that the use of pirated software and expired security products in many government organizations is rampant and offsets the effectiveness of technical measures.

Based on the research findings and analysis, a government cybersecurity framework is proposed, highlighting the key areas necessary for improving cybersecurity in government organizations. It is hoped that the outcomes and findings of this research will benefit other ICT emerging countries.