Evaluating Cybersecurity Awareness in Sri Lankan Healthcare Sector: A Role-Based Training Framework for Public and Private Institutions

Hewamanna I.U.K
(Reg. No.: MS24015844)

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN CYBER SECURITY

December 2025

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

_____

Dr, Junius Anjana

Approved for MSc. Research Project:

_____

MSc in Cyber Security Programme Co-ordinator, SLIIT

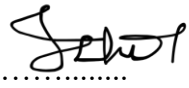
Approved for MSc:

_____

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign: 

Ishanthi Hewamanna

Date: November 2nd 2025

ABSTRACT

Evaluating Cybersecurity Awareness in Sri Lankan Healthcare Sector: A Role-Based Training Framework for Public and Private Institutions

Ishanthi Hewamanna

MSc. in Cyber Security

Supervisor: Dr. Junius Anjana

December 2025

This study investigates cybersecurity awareness within Sri Lanka's healthcare sector and develops a role-based training framework to enhance awareness and secure digital practices across public and private healthcare institutions. As healthcare systems increasingly digitize, human factors remain a major vulnerability, particularly in environments with limited resources and inconsistent policy enforcement.

A quantitative survey was conducted among healthcare professionals to assess their awareness levels, training exposure, institutional support, and perceptions of cybersecurity importance. Data collected through Google Forms were analyzed using Excel and Jamovi. Descriptive statistics, Independent Sample T-Tests, One-Way ANOVA, and Regression Analysis were employed to explore patterns and relationships across professional roles and institution types. Results revealed moderate awareness levels overall, with significant variation between public and private institutions and across roles, emphasizing the need for contextualized, role-specific training. Based on these findings, a Role-Based Cybersecurity Awareness and Training Framework was developed, aligned with NIST SP 800-50r1, the Personal Data Protection Act (2022), and Ministry of Health Information Security Guidelines (2023). Expert evaluation (n = 6) rated the framework highly for clarity, practicality, and policy alignment (mean score = 4.37/5).

The study concludes that micro-learning modules, continuous reinforcement, and leadership involvement can significantly enhance cybersecurity culture in healthcare while minimizing operational disruption. The proposed framework offers a feasible, low-cost, and scalable model to strengthen human-centered cybersecurity resilience across Sri Lanka's healthcare sector.

ACKNOWLEDGEMENT

I wish to express my sincere appreciation to my supervisor Dr. Junius Anjana and the academic staff of the Sri Lanka Institute of Information Technology (SLIIT) for their guidance and academic support throughout the duration of this study. Their feedback and encouragement were instrumental in shaping the direction of this research.

Special thanks are extended to all the healthcare professionals who participated in the survey and to the experts who contributed valuable insights during the evaluation of the proposed cybersecurity awareness and training framework. Their cooperation and feedback greatly enhanced the relevance and practical contribution of this work.

I am also deeply grateful to those closest to me for their continued encouragement, patience, and understanding throughout this journey. Their steady support and belief in my work provided the motivation and perseverance needed to complete this research successfully.

TABLE OF CONTENTS

List of Figures

List of Tables