



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:



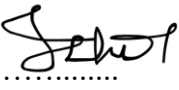
MSc in Cyber Security Programme Co-ordinator, SLIIT

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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

DECLARATION	ii
ABSTRACT.....	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENTS.....	v
List of Figures	viii
List of Tables	ix
Chapter 1 Introduction	1
1.1 Introduction	1
1.2 Research objectives	4
1.3 Research Problem.....	5
1.4 Hypothesis and research questions.....	6
Chapter 2 Literature Review	7
2.1 Cybersecurity Threats in Healthcare	7
2.2 Biggest Cyberattacks on Developing Countries	9
2.3 Digitalization of healthcare sector in Sri Lanka.....	10
2.4 Cybersecurity Awareness in Healthcare Sector	11
2.5 Importance of Role-Based Models in Healthcare Security	13
2.6 Effective Training Delivery Methods	16
2.7 Gap Identification.....	17
Chapter 3 Research Methodology.....	19
3.1 Research Design.....	19
3.2 Sampling Strategy	19
3.3 Data Collection Methods.....	20
3.4 Data Analysis Techniques.....	20
3.5 Conceptual Model	21

3.6 Survey Creation.....	23
Chapter 4 Analysis of survey results	25
4.1 Respondent profiles and demographic	25
4.2 Use of digital technology in healthcare.....	26
4.3 Role-based awareness segmentation	26
4.4 Training exposure and its influence	33
4.5 Institutional support, policies, and culture	35
4.6 Perceived importance and staff attitudes.....	41
4.7 Difference between public and private institutions.....	44
4.8 Inferential Analysis: Differences in Cybersecurity Awareness Across Professional Roles	47
4.9 How the resource difference effect awareness.....	50
4.10 Feedback for a role-based cybersecurity training framework.....	52
Chapter 5 Framework Design and Development.....	56
5.1 Framework Development Approach	56
Role-Based Orientation	57
Integration of Human and Technical Risk Perspectives.....	57
Contextual Adaptation for Sri Lanka.....	57
5.2 Training Awareness Lifecycle	58
Stage 1: Assess and Plan	59
Stage 2: Deliver Training	59
Stage 3: Reinforce and Review	60
5.3 Roles and Responsibilities	60
5.4 Head of the Organization	60
5.5 Training Coordinator.....	61
5.6 System Users.....	62
5.7 Assess and Plan Phase.....	62
5.8 Determination of Scope.....	63

5.9 Segmentation of Audience	63
5.10 Budget	66
5.11 Communication Planning	67
5.12 Development and Delivery Phase	67
5.13 Training and Delivery Principles	67
5.14 Content Development Criteria	68
5.15 Role to Module Mapping	69
5.16 Assessment and Improvement Phase	72
5.17 Evaluation Logic	73
5.18 Checklist Development	73
5.19 Continuous Improvement Cycle	75
Chapter 6 Framework Evaluation: Expert Feedback	76
6.1 Overview of expert panel	76
6.2 Quantitative Evaluation.....	76
6.3 Qualitative feedback analysis.....	77
6.3.1 Implementation challenges.....	77
6.3.2 Recommended Enhancement	78
6.3.3 Summary and Implications.....	78
Chapter 7 Results and Discussion.....	80
7.1 Survey Results: Cybersecurity Awareness and Influencing Factors.....	80
7.2 Expert evaluation of the framework.....	81
7.3 Discussion	82
Chapter 8 Conclusion.....	84
Chapter 9 References	85
Appendix.....	90
9.1 . Appendix 1: Survey Questionnaire	90
9.2 Appendix 2: Expert Feedback Evaluation Survey Questionnaire	95

List of Figures

Figure 1 Conceptual Framework Diagram	22
Figure 2 Survey Reponse: Professional role response	26
Figure 3 Survey Response: Type of institution.....	26
Figure 4 Survey Response: Use of digital technology in healthcare	26
Figure 5 Descriptive Statistics: Current State of Cybersecurity Awareness.....	31
Figure 6 Descriptive Statistics: Current State of Cybersecurity Awareness Plot	32
Figure 7 Training Exposure Sample T-Test.....	35
Figure 8 Institutional Support One-Way ANOVA	40
Figure 9 Institutional Support One-Way ANOVA plot.....	40
Figure 10 Pearson correlation analysis for perceived importance	44
Figure 11 One-way ANOVA result for awareness across roles	48
Figure 12 One-way ANOVA result for awareness across roles - plot.....	49
Figure 13 Regression Analysis of resource effect on awareness	50
Figure 14 Resource effect on institute awareness	51

List of Tables

Table 1 Role Categorization	64
Table 2 Role to Module Mapping	69
Table 3 Evaluation Checklist	73
Table 4 Expert Feedback Summary	76