Evaluating the Efficiency and Effectiveness Of Payment Card Industry Data Security Standard [PCI DSS] In Preventing Payment Card Data Breaches.

Batugedara S.D.
MS23007642.

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

December 2024

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.

_____

Lecturer. Mr. Kanishka Yapa

Approved for MSc. Research Project:

_____

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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

Samudika Danushi Batugedara.

Batugedara S. D.

Date: 01/15/2025

ABSTRACT

Evaluating the Efficiency and Effectiveness of Payment Card Industry Data Security Standard [PCI DSS] In Preventing Payment Card Data Breaches.

Samudika Danushi Batugedara
MSc. in Information Managment
Supervisor: Lecturer Mr. Kanishka Yapa.
December 2024

This paper addresses the growing challenge faced by merchants dealing with credit card transactions which are known to be payment card data breaches and efficiency and effectiveness of payment card industry data security standards.

The Payment Card Industry Data Security Standard (PCI DSS) is a critical framework designed to protect cardholder data and mitigate the risks associated with payment card data breaches. However, despite widespread adoption, the efficiency and effectiveness of PCI DSS in preventing data breaches remains areas of ongoing debate. This study evaluates PCI DSS's role in safeguarding payment card information, focusing on its operational efficiency and ability to prevent breaches effectively.

Very few studies were carried out to evaluate the efficiency and effectiveness of PCI DSS in preventing payment card data breaches. To address this gap, this study will analyze the data on factors affecting the efficiency and effectiveness of PCI DSS in preventing payment card data breaches.

A comprehensive questionnaire was conducted across multiple financial institutions to gather data from security experts on pertinent factors affecting the efficiency and effectiveness of Payment Card Industry Data Security Standard (PCI DSS). This data was meticulously analyzed through a structured analysis using SmartPLS to gauge the effectiveness and efficiency of PCI DSS in thwarting payment card data breaches. The success factors of PCI DSS in preventing data breaches considered in this study are network and system security, data protection, access and identity management, and monitoring and governance. The

findings revealed that the efficiency and effectiveness of PCI DSS in preventing data breaches is critically contingent on these factors. With a statistical significance level set below 0.05, the study highlights how adherence to PCI DSS protocols, combined with robust security practices, substantially enhances data protection.

This research offers profound insights into refining PCI DSS frameworks and supports the enhancement of security measures to boost the safeguarding of payment card information and prevent data breaches.

Also, as the recommendations, after exploring factors affecting the efficiency and effectiveness of PCI DSS in preventing payment card data breaches, the challenges of PCI DSS implementation, asses the applicability and suitability of related security and audit frameworks and proposes recommendations by observing the results and by using the frameworks such as COBIT, ITIL, and ISO 27002 for robust data and information protection.

Ultimately, the study underscores the need for continuous improvement in compliance strategies to address evolving security threats effectively.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who have contributed to the completion of this master's thesis on Evaluating the efficiency and effectiveness of PCI DSS in preventing payment card data breaches.

First and foremost, I am deeply thankful to my research supervisor, Sir Kanishka Yapa, whose guidance, support, and expertise have been invaluable throughout this research journey. His insightful feedback, encouragement, and unwavering dedication have significantly shaped the direction and quality of this thesis.

I am also indebted to Dr. Prasanna Sumathipala, the Dean of Postgraduate Studies at Sri Lanka Institute of Information Technology, whose knowledge and mentorship have enriched my academic experience. Their encouragement and constructive criticism have inspired me to strive for excellence in my research endeavors.

I extend my heartfelt appreciation to the participants of this study, whose willingness to share their insights and experiences has been instrumental in gathering valuable data. Their contributions have provided invaluable perspectives and enriched the depth of analysis in this thesis.

I am grateful to my family and friends for their unwavering support and encouragement throughout this academic journey. Their patience, understanding, and belief in my abilities have been a constant source of motivation.

Finally, I would like to acknowledge the support of security analysts from one of the leading telecommunication organizations and its three subsidiaries for their participation and assistance, which made this research possible. Their support has been instrumental in facilitating the completion of this thesis.

In conclusion, I am deeply grateful to all my colleagues at my organization who have played a part in the realization of this master's thesis. Their contributions have been invaluable, and I am truly appreciative of their support and encouragement.

TABLE OF CONTENTS

DECLARATION ii
ABSTRACT iii
ACKNOWLEDGEMENT v
TABLE OF CONTENTS vi
List of Figures viii
List of Tables ix
Chapter 1 1
1.1 Introduction 1
1.2 Background of the study 2
1.2.1 Payment Card Industry Data Security Standard 3
1.3 Problem Statement 10
1.4 Research Objective 11
1.5 Research Question 12
Chapter 2 13
2.1 Literature Review 13
2.2 Research Gap 27
Chapter 3 30
3.1 Methodology 30
3.1.1 Developing the theoretical framework 32
3.1.2. Theoretical framework. 35
3.2 Research design 36
3.2.2 Conceptual Framework. 38
3.3 Data Collection 55
3.4 Partial Least Square - Structural Equation Modeling (PLS-SEM) 57
3.5 SmartPLS Software 59
3.6 Hypotheses 61
Chapter 4 62
4.1 Interpretation of Results, Findings and Discussion 62
4.2 Measurement Model 63
4.2.1 Factor Loadings 64
4.2.2 Reliability Analysis 66
4.2.3 Construct Validity 67
4.2.3.1. Convergent Validity 68
4.2.3.2. Discriminant Validity 71
4.2.3.2.1. Cross Loadings 72
4.2.3.2.2. Fornell and Larcker Criterion 73
4.2.3.2.3. Heterotrait-Monotrait (HTMT) Ratio 74
4.2.4 . Variance Inflation Factor (VIF) Analysis- Indicator Multicollinearity 75

4.2.5 . Validation of Higher-Order Constructs 77
4.2.6 . coefficient of determination (R^2) 79
4.2.7 . Path Coefficients - Impact on PCI DSS and Data Security 79
4.3 . Structural Model 82
4.3.1 . Path Coefficients and Bootstrapping Results 86
4.3.2 . Bootstrapping Methodology 87
4.3.3 . f-square (f^2) values 88
4.3.4 . Hypotheses Results 90
4.3.5 Aligning the results of the analysis with the research question 93
Chapter 5 95
5.1 . Recommendations. 95
5.1.1 . Integrating Continuous Improvement (CI) Framework to enhance implementation 98
5.1.1.1 Plan-Do-Check-Act (PDCA) Cycle 98
5.1.1.2. Lean Principles 99
5.1.1.3. Six Sigma Methodology 100
5.1.2 Integrating COBIT Principles to Enhance PCI DSS Efficiency and Effectiveness 103
5.1.3 . Integrating ITIL Principles to Enhance PCI DSS Efficiency and Effectiveness 106
5.1.4 . Integrating ISO 27002 with PCI DSS to Enhance Security Governance 109
5.1.5 . Unified Security Governance Framework for PCI DSS 112
5.2 . Summary 115
5.3 . Implications 115
5.4 Conclusion 116
Bibliography 117
Appendix 125

List of Figures

Figure 2.1: Venn Diagram on intersection of two domains 28
Figure 3.1: PCI DSS has twelve requirements divided into four main sectors 32
Figure 3.2: Theoretical Framework 35
Figure 3.4: Relationship between Independent and dependent variables 36
Figure 3.5: Conceptual Framework 38
Figure 4.1: Factor Loadings 65
Figure 4.2: Factor loadings of latent variables 66
Figure 4.3: Construct reliability and validity 67
Figure 4.4: Construct reliability and validity 69
Figure 4.5: Cross Loadings 73
Figure 4.6: Discriminant Validity - Fornell-Larcker criterion 74
Figure 4.7: Discriminant Validity - Heterotrait-Monotrait Ratio (HTMT) – Matrix 75
Figure 4.8: Collinearity Statistics - Variance Inflation Factor (VIF) Analysis 76
Figure 4.9: PLS-SEM results. 78
Figure4.10: Path Coefficients - Matrix 80
Figure 4.11: Path Coefficients - Mean, STDEV, T values, p values 86
Figure 4.12: Bootstrapping Results 88
Figure 4.13: Hypothesis Results 91

List of Tables

Table 1.1: Processes and mechanisms for installing and maintaining network security controls 5
Table 1.2: Network security controls (NSCs) are configured and maintained. 6
Table 1.3: Network access to and from the cardholder data environment (CDE) is restricted. 7
Table 1.4: Network connections between trusted and untrusted networks are controlled. 8
Table 1.5: Risks to the CDE from computing devices that can connect to both untrusted networks and the CDE are mitigated 9
Table 2.1: Existing literature and their resources 13
Table 4.1: Summarized criteria of measurement model 63
Table 4.2: Construct reliability and validity 67
Table 4.3: Average variance extracted. (AVE) 70
Table 4.4: Summarized criteria of structural model 82