LEVERAGING THE POWER OF SQA TO ENHANCE SOFTWARE SECURITY

Kuruppu Arachchilage Hashantha Udara Jayasekara

(179114N)

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2020

LEVERAGING THE POWER OF SQA TO ENHANCE SOFTWARE SECURITY

Kuruppu Arachchilage Hashantha Udara Jayasekara

(179114N)

The dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfillment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2020

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

Also, I hereby grant to the University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic, or other media. I retain the right to use this content in whole or part in future works (such as articles or books).

………………………………. …………………

K.A.H.U. Jayasekara Date:
Signature of the Candidate

The above candidate has carried out research for the Master's thesis under my supervision.

……………………………….. …………………

Dr. Shantha Fernando Date:
Signature of the Supervisor

COPYRIGHT STATEMENT

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

31/05/2020

ABSTRACT

Software security is a growing concern for all ICT organizations since security breaches continue to make headline news. Since the Software Quality Assurance (SQA) professionals are responsible for validating the adherence to software product standards, processes, and procedures, getting them involved can help to solve most of the problem that harms most software development organizations today. Most of the experts involved in the software security industry spend much time discussing how to create secure software. Still, only a few explain how to achieve the goal of successful software security testing. As a result, SQA professionals face many problems in today's dynamic software environments. Organizations pressure them to certify software systems for security, but give little or no detailed advice on how to achieve that objective. It is essential to identify those problems and take the necessary actions to overcome those problems to thrive in the competitive business market so that this research intention is to find out a strategy that can use to develop the security testing mindset of SQA professionals by identifying the significant problems they are facing in software security testing and providing suitable suggestions/recommendations to overcome those problems.

For the research, we used qualitative content analysis research methodology. The survey questionnaires and interviews were conducted to collect data. The preliminary survey was conducted to determine the list of problems that SQA professionals face in software security testing. With the results of the initial study, an online survey was distributed to filter out significant problems. The online survey was shared among different leading IT companies. Lack of specialized SQA people in security testing, Budget, Lack of knowledge about security testing fundamentals, Lack of detailed information and advice, and No security testing training were some of the significant problems identified during the survey. With the results of the survey, a set of follow up interviews been carried with several senior SQA experts to sees their perspective on identified problems. Form a dedicated QA security taskforce to develop and retain the security testing mindset among SQA professionals, Maintain a security testing knowledge portal, Allocate sufficient funds in the budget to provide proper SQA resources and Familiarize and adapt security testing fundamentals, protocols, tools, and methods to fit within existing processes were some of the suggestions made by the domain experts, which they have successfully tried while addressing those problems.

This research delivers several valuable results that can be useful for SQA professionals to grow in software security testing gradually. By properly adopting the strategy, we expect to develop the security testing mindset of SQA professionals inside the organization as well as the industry as a whole. Improved SQA professionals will enhance software security.

ACKNOWLEDGMENT

I need to expose my true thankfulness to everybody who pushed for the successful completion of my research study on "Leveraging the power of SQA to enhance software security."

Primarily, I acknowledge my supervisor, Dr. Shantha Fernando, for the direction and support provided during the research study. Also, I would like to thank Dr. Shehan Perera, Head of the CSE department and Dr. Dilum Bandara, the former coordinator of the MBA in IT for assistance and teaching, and all other faculty associates in the CSE department at the University of Moratuwa.

Moreover, the tremendous support I got from the software professionals who supported me by filling out the surveys, participating interviews, and discussions are greatly admired. Without your help, this research study is not likely to finish successfully.

Exceptional acknowledgments must go to my mother 'Nilanka' father 'Dayananda' brother 'Dinith' and Sister 'Sasheeka' who continuously understanding of the sacrifices that I had to make this study success.

I'm deeply thankful to my friend, Kasuni Gunasekera, for the encouragement, and full support is given to me throughout this research.

The subsequent research dissertation accomplished with the support of people well-known and unknown to me. Finally, I appreciate those who encouraged me in various ways, even if they were not stated above but helpful for the success of this study.

TABLE OF CONTENTS

DECLARATION I

COPYRIGHT STATEMENT II

ABSTRACT III

ACKNOWLEDGMENT IV

TABLE OF CONTENTS V

LIST OF FIGURES VII

LIST OF TABLES X

LIST OF ABBREVIATIONS XII

1. INTRODUCTION 1

 1.1. Background 1

 1.2. Motivation 2

 1.3. Problem Statement and Research Question 3

 1.4. Research Objectives 3

 1.5. Research Contribution 3

 1.6. Organization of Thesis 5

2. LITERATURE REVIEW 6

 2.1. Software Security Testing 6

 2.2. Importance of Software Security Testing 7

 2.3. Software Security Testing as SQA Profession 8

 2.4. SQA Problems in Software Security Testing 10

 2.5. Overcoming SQA Problems in Software Security Testing 12

 2.6. Strategies Used to Develop the Security Testing Mindset of SQA 14

 2.7. Summary 16

3. RESEARCH METHODOLOGY 17

 3.1. Research Methodology 17

 3.2. Measurement and Measures 19

 3.3. Sampling Design 21

  3.3.1. Population 21

  3.3.2. Sampling Procedure 22

4. DATA ANALYSIS AND INTERPRETATION 23

 4.1. Preliminary Survey Results 23

4.2. Online Survey Results ... 27
4.2.1. Analysis Based on Gender ... 30
4.2.2. Analysis Based on Organization Hierarchy ... 32
4.2.3. Analysis Based on Size of QA Department ... 37
4.2.4. Analysis Based on Company Type ... 40
4.2.5. Analysis Based on Target Market ... 43
4.2.6. Analysis of Identified Significant Problems ... 47
4.3. Interview Results ... 82
4.4. Summary of Results ... 100
5. CONCLUSION AND RECOMMENDATIONS ... 104
5.1. Evaluating the Objectives ... 104
5.2. Summary of Contributions ... 105
5.3. Limitations ... 106
5.4. Recommendations ... 106
5.5. Future Work ... 110
REFERENCES ... 111
APPENDIX A: PRELIMINARY SURVEY QUESTIONNAIRE ... 114
APPENDIX B: ONLINE SURVEY QUESTIONNAIRE ... 116
APPENDIX C: INTERVIEW QUESTIONNAIRE ... 126
APPENDIX D: INTERVIEW RESULTS ... 129

LIST OF FIGURES

Figure 3.1: The research methodology. 18
Figure 3.2: Total ICT workforce by work category (SLICTA, 2013). 22
Figure 4.1: Percentage-wise analysis of problems in the online survey. 29
Figure 4.2: Weighted score analysis of problems in the online survey................................ 30
Figure 4.3: Problems distribution for the male category.. 30
Figure 4.4: Problems distribution for the female category. 31
Figure 4.5: Problems distribution for the engineering category. 33
Figure 4.6: Problems distribution for the tactical management category. 34
Figure 4.7: Problems distribution for the middle management category. 35
Figure 4.8: Problems distribution for the executive management category.......................... 36
Figure 4.9: Problems distribution for QA department size less than 10 categories. 37
Figure 4.10: Problems distribution for QA department size less than 50 categories. 38
Figure 4.11: Problems distribution for QA department size more than 50 categories. 39
Figure 4.12: Problems distribution for the product development category........................... 40
Figure 4.13: Problems distribution for the IT service category. 41
Figure 4.14: Problems distribution for both product development and IT service category.. 42
Figure 4.15: Problems distribution for the overseas category... 44
Figure 4.16: Problems distribution for the local market category... 45
Figure 4.17: Problems distribution for the overseas and local market category. 46
Figure 4.18: The agreeable extent of the participants for the "Lack of specialized SQA people in security testing" as a problem. 48
Figure 4.19: Gender-wise analysis on the distribution of "Lack of specialized SQA people in security testing" in the online survey. 49
Figure 4.20: Organization level-wise analysis on the distribution of "Lack of specialized SQA people in security testing" in the online survey. 49
Figure 4.21: Size of the QA department wise analysis on the distribution of "Lack of specialized SQA people in security testing" in the online survey. 50
Figure 4.22: The agreeable extent of the participants for the 'Budget' as a problem. 51
Figure 4.23: Gender-wise analysis of the distribution of 'Budget' in the online survey. 52
Figure 4.24: Organization level-wise analysis of the distribution of 'Budget' in the online survey. 52
Figure 4.25: Size of the QA department wise analysis on the distribution of 'Budget' in the online survey. 53
Figure 4.26: The agreeable extent of the participants for the 'Lack of knowledge about security testing fundamentals' as a problem. 54
Figure 4.27: Gender-wise analysis on the 'Lack of knowledge about security testing fundamentals' in the online survey distribution. 54
Figure 4.28: Organization level-wise analysis on the 'Lack of knowledge about security testing fundamentals' in the online survey distribution. 55
Figure 4.29: Size of the QA department wise analysis on the 'Lack of knowledge about security testing fundamentals' in the online survey distribution. 55
Figure 4.30: The agreeable extent of the participants for the 'Lack of detailed information and advice' as a problem. 57
Figure 4.31: Gender-wise analysis on the 'Lack of detailed information and advice' in the online survey distribution. 57

Figure 4.32: Organization level-wise analysis of the 'Lack of detailed information and advice' in the online survey distribution. 58
Figure 4.33: Size of the QA department wise analysis on the 'Lack of detailed information and advice' in the online survey distribution. 58
Figure 4.34: The agreeable extent of the participants for the 'No security testing training' as a problem. 60
Figure 4.35: Gender-wise analysis of the 'No security testing training' in the online survey distribution. 60
Figure 4.36: Organization-level wise analysis of the 'No security testing training' in the online survey distribution. 61
Figure 4.37: QA department wise analysis on the 'No security testing training' in the online survey distribution. 61
Figure 4.38: The agreeable extent of the participants for the 'Lack of time' as a problem. 63
Figure 4.39: Gender-wise analysis of the 'Lack of time' in the online survey distribution. 63
Figure 4.40: Organization level-wise analysis of the distribution of 'Lack of time' in the online survey. 64
Figure 4.41: Size of the QA department wise analysis on the 'Lack of time' in the online survey distribution. 64
Figure 4.42: The agreeable extent of the participants for the 'Complexity' as a problem. 66
Figure 4.43: Gender wise analysis of the 'Complexity' in the online survey distribution. 66
Figure 4.44 Organization level-wise analysis of the 'Complexity' in the online survey distribution. 67
Figure 4.45 Size of the QA department wise analysis on the 'Complexity' in the online survey distribution. 67
Figure 4.46: The agreeable extent of the participants for the 'Less SQA involvement in system design, requirement gathering, and code review phases' as a problem. 68
Figure 4.47: Gender wise analysis of the 'Less SQA involvement in system design, requirement gathering, and code review phases' in the online survey distribution. 68
Figure 4.48: Organization level-wise analysis on the 'Less SQA involvement in system design, requirement gathering, and code review phases' in the online survey distribution. 69
Figure 4.49: Size of the QA department wise analysis on the 'Less SQA involvement in system design, requirement gathering, and code review phases' in the online survey distribution. 69
Figure 4.50: The agreeable extent of the participants for the 'Lack of management support' as a problem. 71
Figure 4.51: Gender-wise analysis of the 'Lack of management support' in the online survey distribution. 71
Figure 4.52: Organization level-wise analysis of the 'Lack of management support' in the online survey distribution. 72
Figure 4.53: Size of the QA department wise analysis on the 'Lack of management support' in the online survey distribution 72
Figure 4.54: The agreeable extent of the participants for the 'No project requirements' as a problem. 74
Figure 4.55: Gender-wise analysis of the 'No project requirements' in the online survey distribution. 74
Figure 4.56: Organization level-wise analysis of the 'No project requirements' in the online survey distribution. 75

Figure 4.57: Size of the QA department wise analysis on the 'No project requirements' in the online survey distribution. 75
Figure 4.58: The agreeable extent of the participants for the 'Lack of motivation t' as a problem. 76
Figure 4.59: Gender-wise analysis of the 'Lack of motivation' in the online survey distribution. 77
Figure 4.60: Organization level-wise analysis of the 'Lack of motivation' in the online survey distribution. 77
Figure 4.61: Size of the QA department wise analysis on the 'Lack of motivation' in the online survey distribution. 78
Figure 4.62: The agreeable extent of the 'Lower salary scale compared to other IT professions' as a problem. 79
Figure 4.63: Gender-wise analysis of the 'Lower salary scale compared to other IT professions' in the online survey distribution. 80
Figure 4.64: Organization level-wise analysis of the 'Lower salary scale compared to other IT professions' in the online survey distribution. 80
Figure 4.65: Size of the QA department wise analysis on the 'Lower salary scale compared to other IT professions' in the online survey distribution. 81

LIST OF TABLES

Table 3.1: Mapping problems to the questions. 19
Table 3.2: Mapping suggestions to the questions to overcome problems. 20
Table 4.1: Distribution of the organization levels in the preliminary survey. 24
Table 4.2: Distribution of the organization type in the preliminary survey. 24
Table 4.3: Distribution of the target market in the preliminary survey. 24
Table 4.4: Distribution of the department size in the preliminary survey. 24
Table 4.5: Problems encountered by SQA professionals in software security testing. 25
Table 4.6: Suggestions to overcome the security testing problems faced by SQA professionals. 26
Table 4.7: Distribution of the organization levels in the online survey. 27
Table 4.8: Distribution of the organization type in the online survey. 27
Table 4.9: Distribution of the target market in the online survey. 28
Table 4.10: Distribution of the department size in the online survey. 28
Table 4.11: Distribution of gender in the online survey. 28
Table 4.12: Problems ranking for the male category. 31
Table 4.13: Problems ranking for the female category. 32
Table 4.14: Problems ranking for the engineering category. 33
Table 4.15: Problems ranking for the tactical management category. 34
Table 4.16: Problems ranking for the middle management category. 35
Table 4.17: Problems ranking for the executive management category. 36
Table 4.18: Problems ranking for QA department size less than 10 categories. 37
Table 4.19: Problems ranking for QA department size less than 50 categories. 38
Table 4.20: Problems ranking for QA department size more than 50 categories. 39
Table 4.21: Problems ranking for the product development category. 41
Table 4.22: Problems ranking for the IT service category. 42
Table 4.23: Problems ranking for product development and IT service category. 43
Table 4.24: Problems ranking for the overseas category. 44
Table 4.25: Problems ranking for the local market category. 45
Table 4.26: Problems ranking for the overseas and local market category. 46
Table 4.27: Ranking summary of the identified problems based on demographic data. 47
Table 4.28: Suggestions distribution made to overcome ‘Lack of specialized SQA people in security testing’ problem in the online survey. 50
Table 4.29: Suggestion distribution made to overcome the ‘Budget’ problem in the online survey. 53
Table 4.30: Suggestions distribution made to overcome ‘Lack of knowledge about security testing fundamentals’ problem in the online survey. 56
Table 4.31: Suggestions distribution made to overcome ‘Lack of detailed information and advice’ problem in the online survey. 59
Table 4.32: Suggestion distribution made to overcome ‘No security testing training’ problem in the online survey. 62
Table 4.33: Suggestion distribution made to overcome ‘Lack of time’ problem in the online survey. 65
Table 4.34: Suggestion distribution made to overcome the ‘Complexity’ problem in the online survey. 67
Table 4.35: Suggestion distribution made to overcome ‘Less SQA involvement in system design, requirement gathering, and code review phases’ problem in the online survey. 70

Table 4.36: Suggestions distribution made to overcome ‘Lack of management support’ problem in the online survey... 73
Table 4.37: Suggestion distribution made to overcome ‘No project requirements’ problem in the online survey. 76
Table 4.38: Suggestion distribution made to overcome ‘Lack of motivation’ problem in the online survey. 78
Table 4.39: Suggestion distribution made to overcome ‘Lower salary scale compared to other IT professions’ problem in the online survey. 81
Table 4.40: Summary of online survey problems. 100
Table 4.41: Summary of online survey suggessions. 101
Table 4.42: Mapping of problems with suggestions as to the strategy. 102

LIST OF ABBREVIATIONS

Abbreviation	**Description**
BeEF	Browser Exploitation Framework
CR	Change Request
CWE	Common Weakness Enumeration
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communications Technology
IT	Information Technology
MBA	Master of Business Administration
OWASP	Open Web Application Security Project
POC	Proof of Concept
QA	Quality Assurance
QC	Quality Control
QMS	Quality Management System
Q&A	Question and Answer
ROI	Return on Investment
SANS	SysAdmin, Audit, Network and Security
SDLC	Software Development Life Cycle
SQA	Software Quality Assurance
SQL	Structured Query Language
XSRF	Cross-Site Request Forgery
XSS	Cross Site Scripting
ZAP	Zed Attack Proxy