

University of Southern Queensland
Faculty of Business and Law
School of Information Systems



**Key factors impacting on response time of software
vendors in releasing patches for software vulnerabilities**

A Dissertation submitted by

Arjun K.C.

For the award of
Master of Business Research

2012

Abstract

Software vulnerabilities are a major problem for organizations and society given how pervasive the use of computers and the Internet and networks has become. Computers, the Internet and networks in general are underpinned by operating system software and, increasingly, software applications are integrated with the Internet. In this increasingly complex environment hackers and attackers are more likely to take advantage of software vulnerabilities and exploit operating system software and application software. These software exploitations can result in huge losses to businesses which are highly reliant on computerized systems. Software vendors are responsible for securing these vulnerabilities through software patching. This study examines the effect of the level of criticality of software vulnerabilities, type of software vendor and type of software on the software vendors' response time in releasing software patches once software vendors have been informed of vulnerabilities in their software.

The main theoretical support for this study is software security disclosure theory and an economic model of software security investment. These theories provide a framework for understanding how open source versus proprietary software vendors respond with patches to software vulnerabilities depending on the level of criticality of the software vulnerability and the type of software.

Empirical data was collected from four related software vulnerability databases: SecurityFocus, Open Source Vulnerability Database, National Vulnerability Database and Secunia. These four software vulnerability databases contain archival data about software vulnerabilities which has been rigorously collected and screened. This research focuses on software vulnerabilities that have been recently reported in these software vulnerability databases from 2008 to 2010. To test the hypothesised relationships in the proposed research model, multiple regression analysis is used as the main statistical tool.

Analysis of the archival data confirms that software vendors release patches for software vulnerabilities with a medium level of criticality in a shorter response time

than software vulnerabilities with low and high levels of criticality once the vendor has been informed of the software vulnerability. Open source vendors release patches for open source software vulnerabilities 39% quicker than proprietary source vendors release patches for proprietary software. Patches for operating system software vulnerabilities are released 8% slower than patches for application software vulnerabilities.

This study contributes to the existing knowledge and theory by investigating how the different levels of criticality of software vulnerabilities, the differences between open and proprietary source software vendors and the difference between operating system software and application software impact on the response time of software vendors in releasing patches once the software vendor is informed of software vulnerabilities. The findings of this study also establish that responsible disclosure is a more effective mechanism than full disclosure for determining the response time of software vendors. This study contributes to practice by providing an enhanced understanding of the software vulnerability landscape and the complex process of software vendors' patching behaviour.

Certificate of Dissertation

I certify that the ideas, designs, experimental work, results, analyses, software and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Signature of Candidate

Date

ENDORSEMENT

Signature of Principal Supervisor

Date

Signature of Associate Supervisor

Date

Acknowledgements

I would like to take this opportunity to thank everyone who has provided me with assistance and support for the duration of this study. In particular, I would like to thank the following people who helped me to make this thesis a realisation.

Firstly, I would like to express my gratitude to my Principal Supervisor Dr. Michael Lane for his guidance and useful suggestions throughout the structure and contents of this thesis.

Secondly, I would also like to thank Dr. Jianming Yong, my associate-supervisor, who provided initial support during my research proposal.

Last but not least, I wish to express my deepest sense of gratitude to my beloved wife Dilu KC and my daughter Jasmine KC for their love, encouragement and support and my parents for providing me the academic foundations without which this thesis would not be possible. Similarly, sincere thanks to my loving friends Sanjib Tiwari, Arjun Neupane and Rohini Prasad Devkota for their continuous support, cooperation, encouragement and providing light in dark days.

Table of Contents

Abstract	ii
Certificate of Dissertation	iv
Acknowledgements	v
Table of Contents	vi
List of Tables	ix
List of Figures	xi
List of Appendices	xii
List of Abbreviations	xiii
Chapter 1: Introduction	- 1 -
1.1 Introduction	- 1 -
1.2 Background and Significance of the Study	- 1 -
1.3 Research Problem.....	- 3 -
1.4 Justification for the Research	- 4 -
1.4.1 Contribution to Theory and Existing Knowledge.....	- 6 -
1.4.2 Contribution to Practice	- 7 -
1.5 Methodology	- 7 -
1.6 Structure of Dissertation.....	- 9 -
1.7 Definition of Key Terms	- 10 -
1.8 Delimitations of Scope and Key Assumptions.....	- 12 -
1.9 Conclusion.....	- 12 -
Chapter 2: Literature Review	- 14 -
2.1 Introduction	- 14 -
2.2 Information Security.....	- 16 -
2.2.1 Information Security Components.....	- 17 -
2.3 Software Quality.....	- 19 -
2.4 Software Security Investment	- 22 -
2.5 Software Vulnerabilities.....	- 24 -
2.5.1 Classification of Software Vulnerabilities	- 24 -
2.6 Software Vulnerability Databases and Software Vulnerability Classification	- 30 -
2.6.1 SecurityFocus	- 32 -
2.6.2 Open Source Vulnerability Database.....	- 33 -
2.6.3 National Vulnerability Database.....	- 35 -

2.6.4 Secunia.....	- 38 -
2.7 Software Vulnerability Disclosure	- 39 -
2.7.1 Software Vulnerability Disclosure Debate	- 39 -
2.8 Software Vulnerability Disclosure Policy	- 41 -
2.9 Software Vendors	- 42 -
2.9.1 Proprietary Source Software Vendor.....	- 42 -
2.9.2 Open Source Software Vendors.....	- 43 -
2.9.3 Debate on Open and Proprietary Source Software Vendors.....	- 43 -
2.10 Software Vulnerability Disclosure and Software Patching.....	- 45 -
2.10.1 Open Source versus Proprietary Source	- 45 -
2.10.2 The Level of Criticality of Software Vulnerability.....	- 46 -
2.10.3 Operating System Software versus Application Software.....	- 46 -
2.11 Theoretical Support for this Study	- 47 -
2.12 Research Gaps	- 48 -
2.13 Research Question and Sub Questions	- 50 -
2.14 Conceptual Model	- 51 -
2.15 Hypotheses	- 52 -
2.16 Conclusion.....	- 54 -
Chapter 3: Research Design and Methodology	- 56 -
3.1 Introduction	- 56 -
3.2 Research Paradigm	- 56 -
3.3 Research Design	- 57 -
3.3.1 Research Strategy	- 58 -
3.3.2 Archival Analysis	- 59 -
3.4 Data Collection.....	- 60 -
3.4.1 Data Sources	- 60 -
3.4.2 Sample Generation.....	- 63 -
3.4.3 Measurement.....	- 64 -
3.5 Data Analysis	- 66 -
3.5.1 Descriptive Statistics and the Normality of the Raw Data	- 66 -
3.5.2 Reliability and Validity of Data.....	- 67 -
3.5.3 Hypothesis Testing	- 67 -
3.6 Conclusion.....	- 71 -
Chapter 4: Data Analysis	- 72 -
4.1 Introduction	- 72 -

4.2 Descriptive Statistics of Key Variables in the Proposed Research	- 72 -
4.2.1 Type of Software Vendor	- 72 -
4.2.2 Type of Software	- 76 -
4.2.3 The Level of Criticality of Software Vulnerability.....	- 78 -
4.2.4 Response Time.....	- 86 -
4.3 Testing Underlying Regression Assumptions	- 99 -
4.4 Multiple Regression Result Analysis	- 103 -
4.4.1 Discussion of Results of Hypothesis Tests	- 111 -
4.6 Conclusion.....	- 117 -
Chapter 5: Conclusions	- 119 -
5.1 Introduction	- 119 -
5.2 Summary of this Study	- 119 -
5.2.1 Research Problem	- 119 -
5.2.2 Research Hypotheses	- 121 -
5.2.3 Research Methodology	- 124 -
5.2.4 Conclusions about Descriptive Data Findings.....	- 125 -
5.2.5 Conclusions Concerning Results of Research Hypotheses Tests	- 129 -
5.3 Contribution of this Study	- 130 -
5.3.1 Contribution to Theory	- 130 -
5.3.2 Contribution to Practice.....	- 132 -
5.4 Limitation of this Study.....	- 133 -
5.5 Suggestions for Future Research.....	- 133 -
5.6 Summary	- 134 -
References	- 137 -

List of Tables

Table 2.1 Mapping 19 Sins and Top 10 OWASP Software Vulnerabilities into Eight Kingdoms of Software Vulnerabilities.....	- 25 -
Table 2.2 Intentional and Unintentional Software Vulnerability Taxonomy	- 27 -
Table 2.3 The ‘24 Deadly Sins of Software Security’	- 29 -
Table 2.4 Software Vulnerability Databases.....	- 31 -
Table 2.5 Features of SecurityFocus Database	- 33 -
Table 2.6 Features of the Open Source Vulnerability Database (OSVDB).....	- 34 -
Table 2.7 Classification of Software Vulnerabilities in OSVDB by Attack Type	- 35 -
Table 2.8 Features of National Vulnerability Database (NVD).....	- 36 -
Table 2.9 Comprehensive Classification of 23 Specific Types of Software Vulnerabilities	- 37 -
Table 2.10 Features of Secunia Database	- 38 -
Table 3.1 Relevant Situations for Different Research Strategies.....	- 59 -
Table 3.2 OSVDB Data Fields, NVD Data Fields, Secunia Data Fields plus Fields calculated for this Research	- 62 -
Table 3.3 Number of Software Vulnerabilities Documented in OSVDB from SecurityFocus.....	- 63 -
Table 3.4 Criticality Measurement of Software Vulnerabilities	- 65 -
Table 3.5 Software Vulnerability Criticality Metrics	- 66 -
Table 4.1 Distribution of Software Vulnerabilities by Type of Software Vendor	- 73 -
Table 4.2 Types of Software Vulnerability across Software Vendor Type	- 75 -
Table 4.3 Distribution of Software Vulnerabilities across Type of Software.....	- 76 -
Table 4.4 Types of Software Vulnerability across Software Type	- 77 -
Table 4.5 Distribution of Software Vulnerabilities related to the Level of Criticality Categories.....	- 78 -
Table 4.6 Descriptive Statistics of the Level of Criticality of Software Vulnerability.-	78 -
Table 4.7 Level of Criticality across Software Vendor Type	- 80 -
Table 4.8 Variations of Means for Level of Criticality of Software Vulnerabilities across Software Vendor Type	- 81 -
Table 4.9 ANOVA Analysis of Level of Criticality of Software Vulnerability across Type of Software Vendor.....	- 81 -
Table 4.10 Level of Criticality across Type of Software	- 82 -
Table 4.11 Variations of Level of Criticality across Type of Software	- 82 -
Table 4.12 ANOVA Analysis of Level of Criticality of Software Vulnerabilities across Type of Software.....	- 83 -
Table 4.13 Level of Criticality across Response Time	- 83 -
Table 4.14 Types of Software Vulnerability across Level of Criticality of Software Vulnerability	- 85 -
Table 4.15 Distribution of Software Vulnerabilities across Response Time	- 86 -
Table 4.16 Descriptive Statistics for the Response Time	- 87 -

Table 4.17 Results of Descriptive Statistics for the Variable Response Time after Log Transformation	- 89 -
Table 4.18 Response Time across Software Vendor Type	- 92 -
Table 4.19 Response Time across Software Type	- 93 -
Table 4.20 Types of Software Vulnerability across Response Time	- 94 -
Table 4.21 Types of Software Vulnerabilities across Response Time for Open Source Vendor informed Software Vulnerabilities	- 96 -
Table 4.22 Types of Software Vulnerabilities across Response Time for Proprietary Source Vendor informed Software Vulnerabilities	- 97 -
Table 4.23 Level of Criticality across Response Time	- 98 -
Table 4.24 Normality Test for the Proposed Model	- 101 -
Table 4.25 Test for any Extreme Cases which may be an Outlier $< \pm 2$	- 102 -
Table 4.26 Test for any Extreme Cases which may be an Outlier $< \pm 3$	- 102 -
Table 4.27 Summary of Proposed Model Test	- 104 -
Table 4.28 Coefficients Test of Independent Variables in the Proposed Research Model	- 105 -
Table 4.29 Response Time across Software Vendor Type	- 110 -
Table 4.30 Response Time across Software Type	- 110 -
Table 4.31 Summary of Hypotheses Tests and Results	- 111 -
Table 5.1 Three Levels of Criticality Beta Coefficients and Level of Significance for Three MRA ran for Hypothesis H1	- 122 -
Table 5.2 Supported and Unsupported Hypotheses of This Study	- 123 -

List of Figures

Figure 1.1 The Proposed Research Model for this Study	- 8 -
Figure 2.1 Topics Reviewed in Software Vulnerability Disclosure and Software Patching.....	- 15 -
Figure 2.2 Three Classic Principles of Information Security.....	- 17 -
Figure 2.3 Rules of Software Security in SDLC.....	- 21 -
Figure 2.4 Key Factors impacting on Response Time	- 54 -
Figure 3.1 Research Design	- 58 -
Figure 3.2 Multiple Regression Model for this Study	- 69 -
Figure 4.1 Top 12 Software Vendors by Number of Software Vulnerabilities in this Study (from 2008 to 2010).....	- 73 -
Figure 4.2 Types of Software Vulnerabilities by Percentage Terms in this Study-	74 -
Figure 4.3 Box Plot for the Level of Criticality of Software Vulnerability	- 79 -
Figure 4.4 Normal Q-Q Plots for the Level of Criticality of Software Vulnerability...-	80 -
Figure 4.6 Box Plot of the Response Time	- 88 -
Figure 4.5 Normal Q-Q Plot of the Response Time.....	- 88 -
Figure 4.7 Frequency Distribution of Log (Response Time).....	- 90 -
Figure 4.8 Box plot of Log (Response Time)	- 90 -
Figure 4.9 Normal Q-Q Plot of Log (Response Time)	- 91 -
Figure 4.10 Scatter Plot of Regression Standardized Predicted Value	- 99 -
Figure 4. 11 Normal P-P Plot of Regression Standardised Residual	- 100 -
Figure 4. 12 Histogram of Regression Standardised Residual.....	- 101 -
Figure 4.13 Multiple Regression Model for this Proposed Study.....	- 103 -
Figure 4.14 The Resulting Multiple Regression Model.....	- 107 -
Figure 5.1 Research Model and Results of Hypotheses Tests using MRA	- 122 -

List of Appendices

Appendix A - The MRA Test for Three Levels (Low, Medium and High) of
Criticality of Software Vulnerabilities - 151 -

List of Abbreviations

NVD:	National Vulnerability Database
OSVDB:	Open Source Vulnerability Database
CERT:	Computer Emergency Response Team
OWASP:	Open Web Application Security Project
OVAL:	Open Vulnerability and Assessment Language
CWE:	Common Weakness Exposure
CVE:	Common Vulnerability Exposure
CAPEC:	Common Attack Pattern Enumeration and Classification
SDLC:	Software Development Life Cycle
CASE:	Computer Aided Software Design
ERP:	Enterprise Resource Planning
S-SDLC:	Software Security Development Life Cycle
SOAP:	Simple Object Access Protocol
OSGi:	Open Services Gateway Initiative
WASC:	Web Application Security Consortium
XSS:	Cross Site Scripting
CSRF:	Cross-Site Request Forgery