IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY

Enabled Information Small-Medium Enterprises (TEISMES)

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SECURITY IN E-LEARNING by Edgar R. Weippl; ISBN: 0-387-24341-0
IMAGE AND VIDEO ENCRYPTION: From Digital Rights Management to Secured Personal Communication by Andreas Uhl and Andreas Pommer; ISBN: 0-387-23402-0
INTRUSION DETECTION AND CORRELATION: Challenges and Solutions by Christopher Kruegel, Fredrik Valeur and Giovanni Vigna; ISBN: 0-387-23398-9
THE AUSTIN PROTOCOL COMPILER by Tommy M. McGuire and Mohamed G. Gouda; ISBN: 0-387-23227-3
ECONOMICS OF INFORMATION SECURITY by L. Jean Camp and Stephen Lewis; ISBN: 1-4020-8089-1
PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC KEY CRYPTOGRAPHY by Song Y. Yan; ISBN: 1-4020-7649-5
SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang; ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
APPLICATIONS OF DATA MINING IN COMPUTER SECURITY edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3

Additional information about this series can be obtained from http://www.springeronline.com

IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY

Enabled Information Small-Medium Enterprises (TEISMES)

by

Charles A. Shoniregun
University of East London, UK

Springer

Charles A. Shoniregun
University of East London
School of Computing & Technology
Dagenham, Essex
RM8 2AS, UK

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY
Enabled Information Small-Medium Enterprises (TEISMES)
by Charles A. Shoniregun

Advances in Information Security Volume 17

ISBN-10: 0-387-24343-7 e-ISBN-10: 0-387-26334-9
ISBN-13: 978-0-387-24343-6 e-ISBN-13: 978-0-387-26334-2

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11363569, 11500285

springeronline.com

DEDICATIONS

To my Beauty Queen and my Angels

TABLE OF CONTENTS

Dedications v
List of Figures ix
List of Tables xi
List of Contributors and Organisations xiii
Preface xv
Acknowledgements xvii
Chapter 1
Research Overview and Technologies for Internet security 1
1. Introduction 1
2. Research Rationale 2
3. Research Hypothesis 3
4. Conceptual Research Context 5
5. TEISMEs Business Operational Risks 12
6. Technology for Internet Security 14
7. Summary of Chapter One 31
References 32
Chapter 2
Impacts of TEI on SMEs 35
1. Introduction 35
2. Impacts of TEI on SMEs in the UK 35
3. Disintermediation and Reintermediation 40
4. Promote Products to Suit Each Individual Customer 41
5. Electronic Payment 42
6. Generic Problems with Network Protocol Layers 43
7. Application Security Problems 48
8. Summary of Chapter Two 55
References 56
Chapter 3
Risk Assessment of TEI on TEISME 59
1. Introduction 59
2. Concept of Risk 60
3. Risk and the Risk Assessment Approaches 63
4. Quantitative Approaches 68
5. Qualitative Risk Assessment Model 72
6. WEAKNESSES OF RISK ASSESSMENT MODELS 76
7. Why BS7799 76
8. Summary of Chapter Three 79
References 79

Chapter 4
Methodology 83
1. Introduction 83
2. Method 83
3. Shoniregun Risk Assessment Model 94
4. Analysis of Shoniregun's Risk Assessment Model Implementation 100
5. Summary of Chapter Four 102
References 103
Chapter 5
Analysis of Results 105
1. Introduction 105
2. Analysis of 500 TEISMEs Based on co.uk Service Provider 105
3. Laboratory Experiments 109
4. Analysis of 400 TEISMEs Questionnaire Survey 113
5. Correlation Between Annual Sales and Vulnerability 132
6. Analysis of TEISMEs Interviewed 135
7. Analysis of Case Study Observations 138
8. Shoniregun TEISME Risk Assessment Calculation 138
9. Result Summary of Hypotheses Test 146
10. Summary of Chapter Five 146
References 148
Chapter 6
Critical Evaluation and Discussion 149
1. Introduction 149
2. Challenges of TEI on Information Security 149
3. Shared Threats 151
4. TEISMEs Business Operations are not Immune to Internet Attacks 157
5. Risks and Trust 159
6. TEISME Business Operational Risk Liability 163
7. Current Developments in Internet Security 166
8. Government Concern Over Security 171
9. Summary of Chapter Six 174
References 175
Chapter 7
Conclusion 179
1. Global Issues and Internet Security Facing TEISMEs 179
2. Recommendations 187
3. Future Work 190
References 190
Index 193

LIST OF FIGURES

Figure 1–1. Amalgamation of TEI and SMEs 11
Figure 1–2. Trends in Internet take-up among UK SMEs 12
Figure 2–1. The framework model of the impact of TEI on SMEs 36
Figure 2–2. Disintermediation is reintermediation by Internet-eC 40
Figure 2–3. Generic program structure of a virus 48
Figure 2–4. Network security problems according to US enterprises security proffesional 51
Figure 2–5. Number of unique phishing attacks per month (December 2003–June 2004) 52
Figure 2–6. Threats that US IT professionals feel their networks are least protected against 53
Figure 3–1. Three stages of GAMM method 62
Figure 3–2. E-Risk radar 64
Figure 3–3. Proportion of UK businesses that are aware of the contents of BS7799 78
Figure 3–4. Threat, vulnerability and asset parameters 79
Figure 4–1. Overview of Shoniregun's TEISME risk assessment model and calculation 98
Figure 4–2. Breakdown of Shoniregun's TEISME risk assessment model ... 99
Figure 5–1. Common risk encountered by TEISME within their business operations 110
Figure 5–2. Replay Attack 111
Figure 5–3. Screenshot 1. Display Configuration for packets captured 112
Figure 5–4. Screenshot 2. Display detail information of users 112
Figure 5–5. TEISMEs annual sales 119
Figure 5–6. Number of staff employed 119
Figure 5–7. Industrial sector 120
Figure 5–8. Industrial classification 121
Figure 5–9. Survey questionnaire participants 121
Figure 5–10. Types of TEI use by TEISMEs 122
Figure 5–12. Internet safety 123
Figure 5–11. Impacts of TEI on business operation 123
Figure 5–13. Type of TEI used in business transactions 124
Figure 5–14. Identify critical risk exposures 124
Figure 5–15. Risk assessment framework 125
Figure 5–16. Risk improvement process 126
Figure 5–17. Monitoring business risks 126
Figure 5–18. Risk improvement 127
Figure 5–19. Identifying new risks 127
Figure 5–20. Quantifying risks 127
Figure 5–21. Methods for managing the Internet-eC 128

Figure 5-22. How secure is TEISMEs business operation 129
Figure 5–23. Insuring TEISMEs business operations.................................. 130
Figure 5–24. Total vulnerability coefficient.. 133
Figure 5–25. Cost of vulnerabilities encountered by CSO A....................... 142
Figure 5–26. Cost of vulnerabilities encountered by CSO B....................... 143
Figure 5–27. Cost of vulnerabilities encountered by CSO C....................... 145
Figure 5–28. Comparative vulnerability analysis 146
Figure 6–1. Security problems of credit cards and viruses (% Internet users) 150
Figure 6–2. DTI Information security breaches survey 2002...................... 151
Figure 6–3. Merchants' view of online fraud trends.................................... 152
Figure 6–4. Combining common Internet security technologies with biometrics... 169

LIST OF TABLES

Table 1–1. Bolton Committee classification of small firm or SME 9
Table 1–2. EU Definition of SME 10
Table 1–3. Table of biometric technologies 30
Table 1–4. Table of the financial institutions currently using biometrics 31
Table 2–1. An Increase importance of Intermediation Services 39
Table 2–2. Classification of Internet viruses 49
Table 2–3. Number of unique phishing attacks 50
Table 3–1. Parameters for cost of impact and frequency of occurrences 68
Table 3–2. Weaknesses of the selected models 77
Table 5–1. Comparison between Traditional SMEs and TEISMEs 106
Table 5–2. Classification and Taxonomy of TEISMEs business operations 107
Table 5–3. Types of TEISMEs identified within co.uk service provider 108
Table 5–4. Test log result. Total tests performed 250 109
Table 5–5. TEISMEs Questionnaire survey distribution frequency 113
Table 5–6. Absolute and relative frequency of questionnaire feedback 115
Table 5–7. Unforeseen vulnerabilities encountered by TEISME 125
Table 5–8. Security control measures 129
Table 5–9. Suggestions for possible solutions to TEISMEs' business operations 131
Table 5–10. Sales figure and vulnerabilities encountered 132
Table 5–11. Vulnerability coefficient (vulnerabilities per £1m) 133
Table 5–12. Correlation between annual sales and vulnerability coefficient 134
Table 5–13. Identified problems domain of TEISME's business operations 134
Table 5–14. The breakdown of 6 TEISMEs interviewed responses 135
Table 5–15. Risks incurred by CSO A 139
Table 5–16. Risks incurred by CSO B 139
Table 5–17. Risks incurred by CSO C 139
Table 5–18. Classifications of TEISMEs business operations problem domains 140
Table 5–19. Summary of hypotheses tested and results 147
Table 6–1. Average cost of worst security incident 158
Table 7–1. Examples of predictive indices 188

LIST OF CONTRIBUTORS AND ORGANISATIONS

Alex Logvynovskiy e-Centre for Infonomics; London South Bank University

Sonny Nwankwo University of East London, UK

Kasim Charhabagi University of East London, UK

Harvey Freeman Booz Allen Hamilton Inc.

Paul Smith University of East London, UK

Mohammad Saad University of the West of England

Ken Ife The Technology Centre, UK

Jen-Yao IBM T.J. Watson Research Center, USA

Liang-Jie Zhang IBM T.J. Watson Research Center, USA

Vyacheslav Grebenyuk Ukrainian Association for Distant Education, Ukraine

Patrick Hung University of Ontario Institute of Technology, Canada

Ioannis Chochliouros Hellenic Telecommunications Organisation SA, Greece

Max Stempfhuber GESIS, Social Science Information Centre, Germany

Ziyang Duan Reuters America, USA

Subhra Bose Reuters America, USA

AT&T

Dell

Hewlett-Packard Labs

UK Department of Trade and Industry (DTI)

Microsoft Research

AOL

British Telecommunication

eBay

Lucent Technologies

Intrusion.com

Counterpane Internet Security Inc.

University of Massachusetts

CERT Coordination Centre

Computer Virus Consulting Ltd.

National Institutes of Standards and Technology

National Security Agency

Ernst & Young

Sun Microsystems, Inc.

Honeywell

Pricewatercooperhouse

VeriSign Inc.

PREFACE

This study investigates the impacts and risk assessment of technology-enabled information (TEI), which are engaged in the process of discovering the opportunities and challenges presented by TEI to the new form of small medium enterprises (SME) business transactions: Technology Enable Information Small Medium Enterprises (TEISME). Within the UK economy, the notion of TEISMEs is one that forms the focus for this research. Other technologies that enabled information are also discussed. For example electronic mail (e-mail), voice mail, facsimile machines (fax), teleconferencing, data conferencing, video conferencing, electronic data interchange (EDI), and mobile phone (WAP), which are geared towards ease of transferring information are investigated. The electronic marketplace itself can be described as an on-line location for buyers and sellers to meet and conduct their business and complete transactions.

This study identified ways of minimising the risk liability of TEISME business operations as a result of their dependences on TEI (Internet-eC). The rapid evolution and spread of information technology (IT) during the last few years is challenging SMEs, governments and the Internet security professionals to rethink the very nature of risk exposure. Parallel to this notion is the task of identifying: the technologies for Internet Security, the generic problems with network protocol layers, and key elements or threads that might be common to all TEISMEs business operations.

However, the study has revealed that there is an urgent need for a risk assessment model that can be applied to TEISME business operational risks. It has also been found that it is necessary for all TEISME to identify the products' (goods or services) suitability for Internet-eC. The suitability of any products that may be sold on the Internet-eC is just one factor that needs to be taken into account by TEISME. Many TEISMEs launch Internet-eC websites without thinking through what it will take and how the website will impact on their business operations. Without a solid business plan, regardless of whether the business has an 'e' in front of it or not, the TEISME have already prescribed their own downfall. Nevertheless, a trend is apparently beginning to emerge regarding which commodities sell well electronically and which do not. It appears that the sectors of travel, technology, literature and music are reaping the benefits of online retailing, whilst other sectors are missing out.

Furthermore, the success of the Internet-eC will also depend on a variety of factors independent of the Predictive Model of Internet-eC suitability, such as security and risk assessment of TEISME business operations. It has also been established that the weaknesses in the existing security risk assessment approaches have many delimiting factors, which are problematic in nature.

ACKNOWLEDGEMENTS

Many authors and researchers have produced an inordinately long list of acknowledgements. The list sometimes includes all their family names and friends, other authors, researchers, bookmaker and the milkman. I now know how they felt but only brevity prevents me from imitating these great people.

Thanks to my editor Susan Lagerstrom-Fife, publishing director Jennifer Evans and Rudiger Gebauer for their support. Indeed, those kind reminders and useful comments from Susan and Sharon are all appreciated.

A special thank you to a dear friend, Dr Alex Logvynovskiy of e-Center for Infonomics and London South Bank University, for his ever-ending contribution '—never mind, life always gives a chance'.

My sincere thanks to Professor Sonny Nwankwo '—It's a club', Professor Kasim Charhabagi '—You should be OK', Richard Bottoms '— I know the feelings' (East London Business School, University of East London), Dr Paul Smith '—Well done Charles', Dr Fadi Safieddine '— This is very good contribution' (School of Computing and Technology, University of East London), Dr Mohammad Saad (School of Operational Management, University of the West of England) and Dr Ken Ife (The Technology Centre).

I would also like to acknowledge my appreciation to the following organisations: AT&T, Dell, e-Center for Infonomics, HP, IBM, Microsoft Corp, AOL, British Telecommunications, UK Department of Trade and Industry (DTI), eBay, and Lucent Technologies.

And also special thank you, to all the TEISMEs who voluntarily participated in the survey questionnaire and the TEISMEs directors/managing directors who gave their time to be interviewed and participated in the case study observations. The results of all the survey questionnaire, interviews and case study observations became the cornerstone on which chapter 5 'Results' is based.

Undoubtedly, my reflection to past experiences both in the commercial sector and academia has help to bridge the gap in my understanding of the technology for Internet security and the nature of the problems encountered by TEISME within their business operations.

The time spent in writing this book has been particularly difficult on my family. My absence, irritability and frustration to carry on have often reached uncharted personal heights. Tangential thanks go to my beauty queen and my angels for all their support, of which even the most carefully chosen words cannot adequately represent.

My special appreciation to my mother, this book is a testimony of your lifetime belief, and to the memory of my father, sister, and grandmothers.