MODELLING SEMANTICS OF SECURITY RISK ASSESSMENT FOR BRING YOUR OWN DEVICE USING METAMODELLING TECHNIQUE

ZAMHARIAH BINTI MD ZAIN

A thesis submitted in fulfilment of the requirements for the award of the degree of Master of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JULY 2018
ACKNOWLEDGEMENT

First of all, I am blessed and thankful to the Great Almighty, Allah for giving me the strength and the courage to complete this research. Here, I would also like to express my gratitude to everyone who supported, gave me the motivation and assisted me in completing this work. I would like to express my deep appreciation and indebtedness to my supervisor, Dr. Siti Hajar binti Othman and my co-supervisor, Puan Rashidah binti Kadir for their great collaboration, guidance, help, and endless support for this project. Without their help, I probably could not finish this thesis.

To my family, I am truly thankful and want to express my gratefulness especially for my lovely mother, father, brothers and sisters who always support me and being there for me despite the distance. They always gave me advices, and straightened my focus on study because at times, I felt depressed and lost. Their endless support, compassion and love has brought me the toughness, and conviction in facing allegations and challenges in doing my master.

I also want to express my appreciation and thanks to all my friends for their great companionships during my ups and down. With all truthfulness, they have encouraged, supported and helped me a lot in completing this Master Project. The completion of this research would not be possible without their participation and assistance.
ABSTRACT

Rapid changes in mobile computing devices or modern devices such as smartphones, tablets and iPads have encouraged employees to use their personal devices at workplace. Bring Your Own Devices (BYOD) phenomenon in an enterprise has become pervasive in demand for business purposes. Most organizations practice BYOD as it offers a wide variety of advantages such as increasing work productivity, reducing cost and giving employee’s satisfaction. Despite that, BYOD practices trigger opportunities and challenges for the enterprise if there have no security policies, regulations and management on personal devices. Common BYOD security threats includes data leakage, exposure to malicious malware and sensitive corporates information. In this study, the Security-based BYOD Risk Assessment Metamodel (Security-based BYODRAM), a high-level knowledge structure was proposed for describing Security-based BYOD Risk Assessment domain. Review on thirty-five existing models which comprises of Risk Assessment and BYOD security models was done to identify the important concepts and semantic. Meta Object Facility (MOF) was the metamodeling language used in developing the metamodel. This study contributes a platform of incorporating and sharing of the Security-based BYOD Risk Assessment knowledge and giving solutions in managing BYOD security breaches. Real BYOD scenarios such as the Ottawa Hospital, privacy risks in enterprise and independent schools in Western Australian were used in demonstrating the semantics of proposed metamodel.
ERUBAHAN PESAT DALAM PERANTI PENGKOMPUTERAN MODEN SEPATU TEHON PINTAR, TABLET DAN IPAD TELAH MENGGALAKKAN PEKERJA MENGGUNAKAN PERANTI PERIBADI MEREKA DI TEMPAT KERJA. FENOMENA BAWA PERANTI ANDA SENDIRI (BYOD) DI PERUSAHAAN SEMAKIN MELUAS DIGUNAKAN UNTUK TUJUAN PERNIAGAAN. KEBANYAKAN ORGANISASI MENGAMALKAN BYOD KERANA TERDAPAT PELBAGAI KELEBIHAN SEPERTI PENINGKATAN PRODUKTIVITI KERJA, PENGURANGAN KOS DAN KEPUASAN KEPADA PEKERJA. NAMUN BEGITU, BYOD BOLEH MENCETUSKAN PELUANG DAN CABARAN BAGI PERUSAHAAN JIKA TIDAK ADA POLISI KESELAMATAN, PERATURAN DAN PENGURUSAN PERANTI PERIBADI YANG DIGUNAKAN DALAM SESUHUH ORGANISASI. AMARAN KESELAMATAN DENGAN PELAKSANAAN BYOD UMUMNYA TERMASUK KEBOCORAN DATA, TERDEDAH KEPADA ANCAMAN PERISIAN BAHAYA DAN DATA KORPORAT YANG SENSITIF. DALAM KAJIAN INI, METAMODEL KESELAMATAN BERASaskan PENILAIAN RISIKO BYOD (KESELAMATAN BERASaskan BYODRAM), IAITU STRUKTUR PENGETAHUAN PERINGKAT TINGGI DICADANGKAN UNTUK MENGGAmbARKAN DOMAIN PENILAIAN RISIKO BYOD YANG BERASaskan KESELAMATAN. KAJIAN PADA TIGA PULUH LIMA MODEL SEDIA ADA YANG TERDIRI DARIPADA MODEL PENILAIAN RISIKO DAN MODEL KESELAMATAN BYOD TELAH DJALANKAN UNTUK MENGENAL PASTI KONSEP-KONSEP PENTING DAN SEMANTIKNYA. META OBJEK FASILITI (MOF) ADALAH BAHASA METAMODEL YANG DIGUNAKAN DALAM PEMBANGUNAN METAMODEL. KAJIAN INI MENYUMBANG KEPADA PLATFORM MENGGABUNGKAN DAN BERKONGSI PENGETAHUAN PENILAIAN RISIKO BYOD YANG BERASaskan KESELAMATAN DAN MEMBERI PENYELESAIAN DALAM MENGURUSkan PELANGGANAN KESELAMATAN DALAM BYOD. SENARIO-SENARIO BYOD YANG SEBENAR SEPERTI HOSPITAL OTTAWA, RISIKO PRIVASI DALAM PERUSAHAAN DAN SEKOLAH SWASTA DI AUSTRALIA BARAT TELAH DIGUNAKAN UNTUK MENunjUKAN SEMANTIK METAMODEL YANG DICADANGKAN.
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACKNOWLEDGEMENT</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>LIST OF APPENDICES</td>
<td>xvii</td>
</tr>
<tr>
<td></td>
<td>LIST OF ABBREVIATION</td>
<td>xviii</td>
</tr>
<tr>
<td></td>
<td>LIST OF SYMBOLS</td>
<td>xx</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1.1 Overview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1.2 Problem Background</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1.3 Problem Statement</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.4 Research Aim</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.5 Research Objectives</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>1.6 Research questions, objectives and deliverables</td>
<td>7</td>
</tr>
</tbody>
</table>
1.7 Research Scope 8
1.8 Summary 8

2

LITERATURE REVIEW 9

2.1 Introduction 9

2.2 Bring Your Own Devices (BYOD) 10

2.3 Current Status of BYOD 11

2.4 Main Reasons of BYOD Implementation in Organizations 11

2.5 BYOD Pros and Cons 12

2.6 The Distinctive between Risk Assessment Model and BYOD Security Model. 17

2.7 Existing Models of Security-based BYOD Risk Assessment 18

2.7.1 Existing Models of Risk Assessment 19

2.7.1.1 Fujitsu BYOD Assessment Process Model 19
2.7.1.2 Risk Assessment Process Model 21
2.7.1.3 Conceptual Framework of Information Security 22
2.7.1.4 Security Risk Assessment process 24
2.7.1.5 Risk Management Process 25
2.7.1.6 Cloud Security Risk Assessment Framework 26
2.7.1.7 Risk Management Framework for Cloud 28
Computing Environment

2.7.1.8 Microsoft Corporation 29

2.7.1.9 Information Security Awareness and Information System Security Risk 31

2.7.1.10 Privacy Risk Assessment Metamodel 32

2.7.1.11 Risk Management Process of Online Services Security Framework (OSSF) 33

2.7.1.12 OCTAVE Allegro Roadmap 34

2.7.1.13 Risk Management Process 35

2.7.1.14 Quantitative Impact and Risk Assessment Framework for Cloud Security 37

2.7.1.15 IRAM Process Model Concept 37

2.7.1.16 IT Security Risk Management Process Model 39

2.7.1.17 Online Interactive Risk Assessment (OiRA) 40

2.7.1.18 BYOD Risk Assessment Model 42

2.7.1.19 Expert system for Risk Assessment 42

2.7.1.20 Information Risk Management 44

2.7.2 Existing Models of BYOD Security 45

2.7.2.1 Secure Meta-market Architecture 45

2.7.2.2 BYOD Security Model 47

2.7.2.3 Security for the Enterprise Mobile Device 48
Solution Life Cycle

2.7.2.4 White-List based Security Architecture Model

2.7.2.5 Android Security Framework Model

2.7.2.6 BYODroid Framework Model

2.7.2.7 Security Policy Model

2.7.2.8 Security Systems Engineering Process Model

2.7.2.9 BYOD Security Framework Model

2.7.2.10 Meru BYOD Solution Model

2.7.2.11 Control Objectives for BYOD

2.7.2.12 Information Security Strategies

2.7.2.13 BYOD Policy Architecture

2.7.2.14 Network Access Control (NAC)

2.7.2.15 Mobile Content Management (MCM)

2.8 Semantics of Modelling Languages

2.9 Metadata

2.10 Metamodel

2.11 Meta Object Facility (MOF)

2.12 Metamodelling Development Technique

2.13 The Distinction between Models and Framework

2.14 Research Direction

2.15 Summary
3 RESEARCH METHODOLOGY

3.1 Introduction

3.2 Research Approach

3.2.1 Design Science Research

3.2.2 Phase 1 - Problem Identification

3.2.3 Phase 2 - Metamodel Development and Validation

3.2.4 Phase 3 – Applying Security-based BYOD Risk Assessment Knowledge Representation in Real Scenario

3.3 Summary

4 DEVELOPMENT OF SECURITY-BASED BYOD RISK ASSESSMENT METAMODEL

4.1 Introduction

4.2 Step 1: Identify Risk Assessment Models

4.3 Step 2: Extraction Concepts of Existing Models

4.4 Step 3: Short-listed Concepts

4.5 Step 4: Reconcile Concept

4.6 Step 5: Designate Concepts

4.7 Step 6: Relationship among Concepts

4.7.1 The Result of Initial Metamodel (Security-based BYODRAM Version 1.0)

4.8 Summary
VALIDATION OF SECURITY-BASED BYOD RISK ASSESSMENT METAMODEL

5.1 Introduction 125
5.2 Validating the Metamodel 126
5.3 Validation 1: Expert Review (Face Validity) 126
5.3.1 Result Analysis of Questions (Section B1) 127
5.3.2 Result Analysis of Questionnaire (Section B2) 131
5.3.3 Validated version of Security-based BYODRAM1.1 137
5.4 Validation 2: Tracing 140
5.4.1 The Ottawa Hospital as a sample of Security-based BYOD Risk Assessment Case Study 141
5.4.1.1 Using Security-based BYODRAM1.1 to model Ottawa Hospital problems 142
5.4.2 The Sensitive Data Confidentiality and Integrity Problem in Enterprises as a sample of Security-based BYOD Risk Assessment Case Study 144
5.4.2.1 Using Security-based BYODRAM1.1 to Model Sensitive Data Confidentiality and Integrity Problems in Enterprises on BYOD 145
5.4.3 The Independent Schools in Western Australian as a sample of Security-based
BYOD Risk Assessment Case Study

5.4.3.1 Using Security-based BYODRAM1.1 to model Western Australian Independent School Problems 148

5.5 The Strength of the Security-based BYODRAM1.1 151

5.6 Summary 152

6 CONCLUSION 153

6.1 Introduction 153

6.2 Discussion 154

6.3 Research Achievement 155

6.4 Project Constraint 156

6.4 Contribution of the Research 157

6.5 Future Work and Summary of the Research 159

REFERENCES 160

Appendices A – D 170 - 199
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Research questions, objectives and deliverables</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>Security main aspects of BYOD security requirements</td>
<td>33</td>
</tr>
<tr>
<td>2.2</td>
<td>Layer in Android Security Framework (Fielder, 2013)</td>
<td>36</td>
</tr>
<tr>
<td>2.3</td>
<td>Metamodelling Development Technique</td>
<td>49</td>
</tr>
<tr>
<td>3.1</td>
<td>Expert personnel for validation</td>
<td>87</td>
</tr>
<tr>
<td>4.1</td>
<td>The process of getting the main concepts in each risk assessment</td>
<td>92</td>
</tr>
<tr>
<td>4.1</td>
<td>existing models</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>The process of getting the main concepts in each BYOD security</td>
<td>93</td>
</tr>
<tr>
<td>4.2</td>
<td>existing models</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>Comparison of <strong>Prepare</strong> concepts definitions between existing</td>
<td>99</td>
</tr>
<tr>
<td>4.3</td>
<td>models</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Comparison of <strong>Analyse</strong> concepts definitions between existing</td>
<td>101</td>
</tr>
<tr>
<td>4.4</td>
<td>models</td>
<td></td>
</tr>
<tr>
<td>4.5</td>
<td>Comparison of <strong>Assess</strong> concepts definitions between existing</td>
<td>104</td>
</tr>
<tr>
<td>4.5</td>
<td>models</td>
<td></td>
</tr>
<tr>
<td>4.6</td>
<td>Comparison of <strong>Control</strong> concepts definitions between existing</td>
<td>106</td>
</tr>
<tr>
<td>4.6</td>
<td>models</td>
<td></td>
</tr>
<tr>
<td>4.7</td>
<td>Concepts reconciled are designated into four Security-</td>
<td>109</td>
</tr>
</tbody>
</table>
based BYOD Risk Assessment phases

4.8 UML class relationships 111

4.9 Relationships created among the concepts 113

5.1 The validation techniques used in metamodel validation 126

5.2 Index measured (Johns, 2010). 128

5.3 Analysis of Expert Review based on Likert Scale Questions 129

5.4 List of new added and modified concepts based on the Expert Review Validation Technique 128

5.5 List of added and modifications of relationships between concepts in Security-based BYODRAM1.0 128
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Mobile malware abilities on devices (Symantec, 2011)</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Fujitsu BYOD Assessment Process Model (Fujitsu, 2013)</td>
<td>20</td>
</tr>
<tr>
<td>2.3</td>
<td>Risk Assessment Process Model (Ross, 2012)</td>
<td>22</td>
</tr>
<tr>
<td>2.4</td>
<td>Conceptual Framework of Information Security (Bakhtiyari Shahri, 2012)</td>
<td>23</td>
</tr>
<tr>
<td>2.5</td>
<td>Security Risk Assessment Process (Landoll, 2006)</td>
<td>25</td>
</tr>
<tr>
<td>2.6</td>
<td>The risk management process from ISO 31000:2009. (Purdy, 2010)</td>
<td>26</td>
</tr>
<tr>
<td>2.7</td>
<td>Cloud Computing Risk Assessment Framework (Albakri et al., 2014)</td>
<td>27</td>
</tr>
<tr>
<td>2.8</td>
<td>Risk Management Framework for Cloud Computing Environment (Zhang et al., 2010)</td>
<td>29</td>
</tr>
<tr>
<td>2.9</td>
<td>Microsoft Corporation Framework (Nicholas, 2013)</td>
<td>30</td>
</tr>
<tr>
<td>2.10</td>
<td>Information Security Awareness and ISS Risk Assessment Model (Mejias, 2012)</td>
<td>31</td>
</tr>
<tr>
<td>2.11</td>
<td>Privacy Risk Assessment Metamodel (Friginal et al.)</td>
<td>33</td>
</tr>
<tr>
<td>2.13</td>
<td>OCTAVE Allegro Roadmap (Caralli et al., 2007)</td>
<td>35</td>
</tr>
<tr>
<td>2.15</td>
<td>IRAM Process Model (Neto et al., 2009)</td>
<td>38</td>
</tr>
<tr>
<td>2.16</td>
<td>IT Security Risk Management Process Model (Goldstein and Frank, 2016)</td>
<td>40</td>
</tr>
<tr>
<td>2.17</td>
<td>Online Interactive Risk Assessment (OSHA, 2015)</td>
<td>41</td>
</tr>
<tr>
<td>2.18</td>
<td>BYOD Risk Assessment Model (Tanimoto et al., 2016)</td>
<td>42</td>
</tr>
<tr>
<td>2.19</td>
<td>Expert system for Risk Assessment (Science, 2013)</td>
<td>43</td>
</tr>
<tr>
<td>2.20</td>
<td>Information Risk Management (Carlson et al., 2010)</td>
<td>45</td>
</tr>
<tr>
<td>2.21</td>
<td>SMM concept in BYOD paradigm (Armando, Costa, et al., 2014)</td>
<td>47</td>
</tr>
<tr>
<td>2.22</td>
<td>Security for the Enterprise Mobile Device Solution Life Cycle (Souppaya and Scarfone, 2013)</td>
<td>448</td>
</tr>
<tr>
<td>2.23</td>
<td>White-List based Security Architecture Model (Lee et al., 2013)</td>
<td>549</td>
</tr>
<tr>
<td>2.24</td>
<td>BYODroid Framework Model (Armando et al., 2013)</td>
<td>552</td>
</tr>
<tr>
<td>2.25</td>
<td>Security Policy Model (Bann et al., 2015)</td>
<td>554</td>
</tr>
<tr>
<td>2.26</td>
<td>Security Systems Engineering Process Model</td>
<td>555</td>
</tr>
</tbody>
</table>
2.27 BYOD Security Framework Model (Zahadat et al., 2015) 558

2.28 Meru BYOD Solution Model (Networks, 2013) 660

2.29 Control Objectives for BYOD (Ghosh et al., 2013) 661

2.30 Information Security Strategies (Gallotto and Chen, 2014) 662

2.31 BYOD Policy Architecture (Garba et al., 2015) 664

2.32 Network Access Control (NAC) (Sans, 2013) 665

2.33 Mobile Content Management (MCM) (Romer, 2014) 666

2.34 MOF modeling hierarchy (Karagiannis & Kuhn, 2002) 772

3.1 Research methodology of this research work 80

3.1 TStep-by-Step process of the Security-based BYODRAM Creation 82

4.1 Security-Based BYOD Risk Assessment Model Perspectives 90

4.2 Preparation-phase class of concepts 116

4.3 Analysis-phase class of concepts 118

4.4 Assessment-phase class of concepts 121

4.5 Control-phase class of concepts 123

5.1 TSecurity-Based BYODRAM1.1: A validated version of Preparation-phase concepts 137

5.2 TSecurity-Based BYODRAM1.1: A validated version of Analysis-phase concepts 138
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>TSecurity-Based BYODRAM1.1: A validated version of Assessment-phase concepts</td>
</tr>
<tr>
<td>5.4</td>
<td>TSecurity-Based BYODRAM1.1: A validated version of Control-phase concepts</td>
</tr>
<tr>
<td>5.5</td>
<td>Control Coordination Model (M1), the example of model type which can be instantiated from Security-Based BYODRAM1.1</td>
</tr>
<tr>
<td>5.6</td>
<td>Ottawa Hospital Security Risk Control Coordination Workflow (Real World/Object Model, M0), instantiated from The Administration Coordination Model (Model, M1)</td>
</tr>
<tr>
<td>5.7</td>
<td>Security Risk Assessment Model (M1), derived from Security-Based BYODRAM towards generating Enterprises Security Risk Assessment</td>
</tr>
<tr>
<td>5.8</td>
<td>TE Enterprises Security Risk Assessment Model (Real World/Object Model, M0), instantiated from the Security Risk Assessment Model (Model, M1)</td>
</tr>
<tr>
<td>5.9</td>
<td>Security Risk Control Model (M1), derived from Security-Based BYODRAM towards generating Western Australia Independent School Security Risk Control</td>
</tr>
<tr>
<td>5.10</td>
<td>Western Australia Independent School Security Risk Control Model (Real World/Object Model, M0), instantiated from the Security Risk Control Model (Model, M1)</td>
</tr>
</tbody>
</table>
## LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>List of Set I Model</td>
<td>170</td>
</tr>
<tr>
<td>B</td>
<td>Short-Listed Concepts Of Set I (Thirty-five Existing Models)</td>
<td>179</td>
</tr>
<tr>
<td>C</td>
<td>Relationships Created among the Concepts in Security-based BYODRAM Phases</td>
<td>185</td>
</tr>
<tr>
<td>D</td>
<td>Initially Identified Security-based Byod Risk Assessment Metamodel Concepts and their Definitions</td>
<td>193</td>
</tr>
</tbody>
</table>
### LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASF</td>
<td>Android Security Framework</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Devices</td>
</tr>
<tr>
<td>BYOD SF</td>
<td>BYOD Security Framework</td>
</tr>
<tr>
<td>BYODRA</td>
<td>BYOD Risk Assessment</td>
</tr>
<tr>
<td>BYODRAM</td>
<td>BYOD Risk Assessment Metamodel</td>
</tr>
<tr>
<td>BYOP</td>
<td>Bring Your Own Phone</td>
</tr>
<tr>
<td>BYOPC</td>
<td>Bring Your Own PC</td>
</tr>
<tr>
<td>BYOT</td>
<td>Bring Your Own Technology</td>
</tr>
<tr>
<td>CBA</td>
<td>Cost-Benefit Analysis</td>
</tr>
<tr>
<td>CCs</td>
<td>Cloud Clients</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>EMDSLC</td>
<td>Enterprise Mobile Device Solution Life Cycle</td>
</tr>
<tr>
<td>IRAM</td>
<td>Information Risk Assessment Methodology</td>
</tr>
<tr>
<td>IRM</td>
<td>Information Risk Management</td>
</tr>
<tr>
<td>ISA &amp; ISS RA</td>
<td>Information Security Awareness and Information System Security Risk Assessment</td>
</tr>
<tr>
<td>IT SRM</td>
<td>Information Technology Security Risk Management</td>
</tr>
<tr>
<td>MAM</td>
<td>Mobile Application Management</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MCM</td>
<td>Mobile Content Management</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>MIF</td>
<td>Model Important Facility</td>
</tr>
<tr>
<td>MOF</td>
<td>Meta Object Facility</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>Operationally Critical Threat, Asset, and Vulnerability Evaluation</td>
</tr>
<tr>
<td>OiRA</td>
<td>Online Interactive Risk Assessment</td>
</tr>
<tr>
<td>OMG</td>
<td>Object Management Group</td>
</tr>
<tr>
<td>OSSF</td>
<td>Online Services Security Framework</td>
</tr>
<tr>
<td>PRA</td>
<td>Privacy Risk Assessment</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>RAP</td>
<td>Risk Assessment Process</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>RMP</td>
<td>Risk Management Process</td>
</tr>
<tr>
<td>SMM</td>
<td>Secure meta-market</td>
</tr>
<tr>
<td>SPM</td>
<td>Security Policy Model</td>
</tr>
<tr>
<td>SRA</td>
<td>Security Risk Assessment</td>
</tr>
<tr>
<td>SRAF</td>
<td>Security Risk Assessment Framework</td>
</tr>
<tr>
<td>SSEP</td>
<td>Security Systems Engineering Process</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modeling Language</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WLSA</td>
<td>White-List Security Architecture</td>
</tr>
</tbody>
</table>
LIST OF SYMBOLS

\( \bar{w} \) - Weighted average
\( w \) - Weight of the item
\( x \) - Values of the items
\( N \) - Sum of weight of the item
\( \Sigma \) - Sum
CHAPTER 1

INTRODUCTION

1.1 Overview

*Bring Your Own Devices* (BYOD) refers to a concept of allowing employees to use their own mobile devices such as smartphones, tablets, laptops and iPads for work purposes. Since 2012, the use of personal devices at workplace has become pervasive (Jamaluddin et al., 2015). Many organizations implemented BYOD in their information technology management and it is increasing from time to time. BYOD allows employees to bring and use their own devices at work. In addition, BYOD usage is a good practice in many enterprises nowadays, since it can increase the quality of work, comfort and reduce cost for IT infrastructure management. However, even though BYOD brings many advantages in organization, there are also BYOD security issues faced by the employees. This caused challenges and difficulties to the security experts to manage the information of BYOD security (Fiorenza, 2014). Therefore, metamodelling technique has been chosen as the solution to structure and manage the knowledge of BYOD security risk. Security-based BYOD Risk Assessment Metamodel (BYODRAM) has been proposed to minimize the BYOD security problems in enterprises.
1.2 Problem Background

BYOD phenomenon is currently becoming more prevalent in the business industry and certain organizations. Based on the survey in Asia Pacific, there are more than 85% Malaysians who used their own devices at workplace and only 26% of them were provided with sufficient facilities by their IT department. Employees can also create, store, and manage the corporate data using the devices. Various types of personal devices used by employees at workplace such as smartphones, tablets, IPad, and laptops caused lots of security problems and until now there are no comprehensive guideline that could handle security risk in BYOD devices. Guidelines are general statements that are used in making achievement in the policy objectives (Souppaya and Scarfone, 2013). This is done by providing a framework to implement procedures.

Based on the research made, it is found that there is also faults with the existing models in assessing the BYOD risks. The existing models are developed to manage the risks but there are no exact Security-based BYODRAM that is developed to manage the BYOD security issues. There is a question on how to manage BYOD issues and challenges in enterprises (Shumate and Ketel, 2014). Based on this, the operational risk management should be implemented to avoid the operational risks since the operational risk may impact the implementation of strategic decisions. This includes the identifying, measuring, monitoring, reporting, controlling and mitigating the process. The analysis is also needed to determine the cost to fix operational risk problems and the loss due to the operational risk event (Basel Committee on Banking Supervision, 2001). Hence, it is a necessity to create generic representation of the knowledge in managing BYOD security risks. Therefore, metamodelling technique is found suitable in managing the knowledge of BYOD Risk Assessment (Othman, 2012).

One of the biggest problems related to BYOD adoption is data leakage. This is caused by corporate data that can be accessed through Wi-Fi connection and the transmission of data which is also not encrypted. The loss of mobile devices due to theft is the biggest risk by adopting BYOD that could be faced by enterprises
(AlHarty and Shawkat, 2013). If the employee lose their personal devices that stored corporate data, it can cause untrusted parties to retrieve all the private data inside the device (Wiech, 2013). All the sensitive information inside the devices might be accessed by the intruders and taken for specific purpose. Other than that, factor that contributes to data leakage is when the employee quit job from the company and it has high possibilities that the corporate data still remain inside their own devices (Wiech, 2013). It also been stated by Forrester (2012), that mobile devices security concerns with 65% is the biggest security challenge by deploying BYOD program. Angwin et al. (2011) mentioned that when employees access the network resource using mobile devices, outsiders can easily trace the personal information and corporate data.

According to the existing models of Security-based BYOD Risk Assessment, there is lacking of unified approach in security risk assessment. For example, one of the existing models which is Risk Assessment Process model which is developed to assess the information security risk (Ross, 2012). This model lacks of the BYOD security main components such as the Mobile Device Management (MDM), policy, access control, remote wiping, antivirus and anti-malware (Downer and Bhattacharya, 2016). So, the Security-based BYODRAM will be developed by integrating the BYOD security and assessment main components within the metamodel. So, this is the reason why an investigation of the existing models of risk assessments and BYOD security is required in order to extract all the main components of risk assessment and BYOD security concepts.

It is important to develop a comprehensive information system that stores and manages the BYOD security related issues. The BYOD domain users will have a knowledge of hazards and the risk level of specific BYOD risks. Besides, this knowledge-based system recommend security controls in handling specific BYOD issues. The organization must have a standard guideline on managing BYOD risk related problems because it requires variety of business process in solving the risks. The complexity of the user to access the knowledge of BYOD security risk will be ease with the metamodel. This proposed metamodel support the user of BYOD domain such as expert, security manager, and officer in making decisions of the related security issues.
BYOD policy is becoming a serious phenomenon when it affects the information security risks of the employer’s information such as report, preserve data and data leakage. BYOD implementation causes greatest challenge in organizations when the confidential data is not managed strategically by the organization itself (Olalere et al., 2015). Referring to this, BYOD policy should complement other information security and governance policies. Personal mobile devices usage among workers causes security issues problem as workers commonly will carry their own devices which contain private and confidential data everywhere (Broomfield, 2006). The security requirement should be provided for mobile devices such as authentication, transmission encryption requirements, wipe devices system, right to manage, monitor and wipe devices, support model, company liability, restrict the usage of devices, acceptable use and practices for mobile data usage on international travel (EY, 2013).

The existing models of Security-based BYOD risks assessment also lacks the BYOD security components in its implementation. Based on the existing models, the protection of internal network resources should be enhanced; for example the Virtual Private Network (VPN), access control, and firewalls. For example, BYOD Security model lacking of security protection within the company network services. It only provides limited security protection in the channel of communication through VPN (Ali et al., 2016). So, this revealed the needs and importance of managing BYOD security knowledge. Due to this, the enhancement of the Security-based BYOD Risk Assessment will be done to ensure the improvement of BYOD security and risk assessment components in assessing risks.

The metamodel technique is chosen in managing the BYOD security risks problems. Based on this, metamodelling is needed in minimizing the BYOD risks. The metamodel plays its role in supporting the engineering design optimization. Intensive research has also been done in deploying metamodelling techniques in design and optimization. Metamodelling can be used in problem formulation. According to this, the metamodel is used to solve the complex domain. Any domain which has shared key-points need metamodelling to integrate it into one platform. Next is metamodelling can play a role in model approximation, which is used in approximation of computation-intensive process across the whole design space.
aimed to reduce the computational cost. Besides, metamodelling has the ability to allow modellers to structure, organize, and manage any domain knowledge to solve the interoperability’s issues. (Wang and Shan, 2007).

In addition, malicious malware is also one of the most challenging security risks engaged to BYOD. Adopting BYOD may bring malware and viruses to the company network. Malware is the attack that is based on the malicious applications that are able to affect both the devices and the applications inside devices (Olalere et al., 2015). Mobile malware consists of the applications that is embedded with code inside and compromised with the security of devices (Morrow, 2012). In 2012, there is Shamoon malware that inactivate more than 30,000 computers and also stole data of the national oil company, Saudi Aramco in Saudi Arabia (Armando et al., 2014). In March 2013, at the top three South Korean banks and the country’s two largest broadcaster computer networks were down caused by malicious malware (Fielder, 2013).

Enterprise needs a standard guideline in handling the security risks issues. Based on the review made on the existing models, there are lacking of risk assessment components such as risk specification, risk analysis, and risk evaluation. Risk specification is used to determine the risk factors of BYOD and they are extracted from a comprehensive viewpoint by using the Risk Breakdown Structure (RBS) method. For risk analysis, risk matrix method is used and it consists of four countermeasures in accordance with their probability and risk impact such as risk transferences, risk mitigation, risk acceptance and risk avoidance. For the risk evaluation, it determines the countermeasures based on the risk factors that are investigated (Tanimoto et al., 2016). By using a metamodel form, an integrated view of all important phases involving Security-based BYOD Risk Assessment will be analysed and determined. The security risks which is engaged to the BYOD adoption can be minimized by considering all the important phases in Security-based BYOD Risk Assessment. This is one factor why metamodel is chosen to manage the BYOD risks problems (Othman, 2012).
1.3 Problem Statement

Although BYOD brings advantages, there also security risks impact faced by companies when implementing BYOD. Besides, there are no existing Security-based BYODRAM that can be used as references. So, the appropriate guideline must be strategically developed and implemented to minimize the BYOD risks. The guideline is important for managing the security of BYOD risks. All the important concepts needed in assessing the BYOD risks which is security risk assessment concepts should be considered. This study plans to enhance the security in the risk assessment approach of BYOD risks. Therefore, the questions are how to assess the BYOD risks and what is the appropriate procedure?

The following are research questions of this research:

i) What is the important elements in the Security-based BYOD risk assessment domain?

ii) How to assess BYOD risk with Security-based BYODRAM?

iii) What technique will be used to validate the developed Security-based BYODRAM for assessing BYOD risks?

1.4 Research Aim

This research aims to manage knowledge of how security risk assessment in BYOD domain should be conducted through a high level knowledge structure, a metamodel. This approach is important as it could allow domain users in making decisions when they face various types of BYOD risks.
1.5 Research Objectives

The objectives are stated as follows:

i) To identify the security risk assessment important concepts for BYOD domain from existing sources.

ii) To use the metamodelling approach in developing the Security-based BYODRAM in assessing BYOD risks.

iii) To validate the Security-based BYODRAM by using metamodel validation techniques.

1.6 Research Questions, Objectives and Deliverables of this Research

Table 1.1 represents the research questions, objectives and deliverables of this research.

<table>
<thead>
<tr>
<th>Research Question</th>
<th>Objective</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>i) What is the important elements in the Security-based BYOD risk assessment domain?</td>
<td>i) To identify the security risk assessment important concepts for BYOD domain from existing sources.</td>
<td>i) BYOD concepts</td>
</tr>
<tr>
<td>ii) How to assess BYOD risk with Security-based BYODRAM?</td>
<td>ii) To use the metamodelling approach in developing the Security-based BYODRAM in assessing BYOD risks.</td>
<td>ii) BYOD metamodel</td>
</tr>
<tr>
<td>iii) What technique will be used to validate the developed Security-based BYODRAM for assessing BYOD risks?</td>
<td>iii) To validate the BYODRAM by using metamodel validation techniques.</td>
<td>iii) A validated BYODRAM</td>
</tr>
</tbody>
</table>
1.7 Research Scope

The scope of the research is limited to the following, namely:

i) This study focuses on the development of the Security-based BYODRAM with the important elements needed in assessing BYOD risks based on the existing security risk assessment models.

ii) This study focus on the enhancement of the lackings in the existing models in the BYOD security risks context.

iii) This research used two techniques in validating the metamodel to manage the knowledge of BYOD security risks, but in this research, we used the metamodel technique. Two validation techniques are used in validating the proposed Security-based BYODRAM. The first one is Expert Review (Face Validity) and another one is Case Study (Tracing) techniques.

1.8 Summary

In this chapter, the preliminary study for the research has been discussed. The introduction, background and problem of the study was described to give more information and understanding about the research that was conducted. Besides, there was a discussion on project aims and objectives that provided clear information on things that were focused in this research. Next, the project scopes also gave information about the limitations of the research. In the next chapter, discussion is about the literature review which includes the analysis of the existing model collection.
REFERENCES


Document.

frameworks. Proceedings - 2015 Conference on Information Assurance and

computing security management framework. In Cloud Computing (CLOUD),
2011 IEEE International Conference on (pp. 364-371). IEEE.

Angwin, J. and Valentino-Devries, J., 2011. Apple, Google collect user data. The
Wall Street Journal.

for metamodel-based domain specific languages. Formal and Practical

Proceedings of the 28th Annual ACM Symposium on Applied Computing -
SAC '13, p.1852.

your own device” paradigm. Computer, 47(6), pp.48–56.

the use of mobile devices in the operation of critical infrastructures.
Bermell-Garcia, P., 2007. A metamodel to annotate knowledge based engineering codes as enterprise knowledge resources.
CISCO. 2012. CISCO BYOD Smart Solution.


Fielder, Tales from the darkside: Mobile malware brings down Korean banks, RSA Security Analytics, March 21, 2013

Flores, D.A., Bring Your Own Disclosure : An Analysis of BYOD Threats to Corporate Information.


Krehel, O. 2011. Worse than zombies: the mobile botnets are coming.


Lee, K., Tolentino, R. S., Park, G. C., & Kim, Y. T. 2010. A study on architecture of
malicious code blocking scheme with white list in smartphone environment. In *Communication and Networking* (pp. 155-163). Springer Berlin Heidelberg.


Networks, M., BYOD Best Practices.

Nicholas, J.P., Response of Microsoft Corporation to Request for Information. , 98052(425).


Qing, L. Y. (2013). BYOD on rise in Asia, but challenges remain. *ZDNet*.


Sabatier, P.A. et al., 1999. Theories of the Policy Process,

Sans, 2013. “Your Pad or Mine?”


