BRING-YOUR-OWN DEVICE(BYOD) GUIDANCE: INFORMATION SECURITY CONSIDERATIONS AND RECOMMENDATIONS FOR MALAYSIAN ARMY IN PENINSULAR MALAYSIA

BY

FIKRI HANIS BIN MD BADARUDIN

A dissertation submitted in fulfillment of the requirement for the degree of Master of Protective Security Management.

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

MARCH 2022

ABSTRACT

Bring Your Own Device (BYOD) is a new phenomenon in which employees connect their personal mobile devices to an enterprise network to gain access to corporate information and conduct daily business functions. The issues of BYOD and its security has received significant attention; thus, the research is being conducted in order to investigate the use of application of the new and trendy devices which can contributes to as many information, knowledges and connections as the All-in-One concept with the whole countries in the world. Then, BYOD guidance: information security consideration is the title that has been chosen for the research upon all the need and relevancies of the security information and knowledges for the benefits of the country, Malaysia in the midst of sciences and technology era. And, the key words applied in the research such as devices, facilities, security, military forces, etc. The objective of this study is to identify the level of information security consideration on the practice of BYOD in the organization, then, to recognize factors that should be considered in ensuring organization's information is secured while enabling the use of BYOD and to emphasize the security risks which can be related to the use of BYOD in organizations. The respondent will be 200 respondents among the military forces who work in Malaysian Army among personnel of the Markas Pemerintahan Medan Barat Tentera Darat (MK PMBTD). This study uses a quantitative and qualitative research method using SPSS 25.0 to get the data from the respondent. The findings of this study show that Information Security Consideration is moderately and significant with Successful BYOD Practice (r=0.606, p=0.000) and Security Measure Implemented (r=0.711, p=0.000) strongly and significant with Successful BYOD Practice. Then, the Security Risk showed strongly and significant (r=0.720, p=0.000) with Successful BYOD Practice. Then, the Beta coefficient is 0.569, which is the greatest satisfaction with Security Risk and this corresponds with the highest t-statistic of 8.036. The research provides good analytical guidance on the conceptual security maintenance framework for BYOD implementation by enhancing IT security management. The research demonstrated that it is possible to create appropriate IT security model in order to enhance BYOD security management. Hence, through this beneficial approach, it will become an effective way to determine the factors which influence efficiency and effectiveness of BYOD practice.

ملخص البحث

يعد إحضار جهازك الخاص او استخدام جهازك الشخصي في العمل (BYOD) ظاهرة جديدة يقوم فيها الموظفون بربط أجهزتهم الشخصية المحمولة بشبكة المؤسسة للحصول على معلومات الشركة والقيام بوظائف تجارية يومية. حظيت قضايا إحضار جهازك الخاص BYOD وأمنها اهتمام كبير من طرف الخبراء. تم إجراء هذا البحث من أجل التحقيق في استخدام تطبيقات الأجهزة الجديدة والعصرية التي يمكن أن تساهم في العديد من المعلومات والمعارف والصلات مثل مفهوم الكل في واحد (All-in-One) مع جميع البلدان في العالم اولا وبعدها. إرشادات لإحضار الجهاز الخاص او استخدام جهازك الشخصي في العمل. تم اعتبار أمن المعلومات عنوان الذي تم اختياره للبحث في جميع احتياجات المعلومات الأمنية والمعارف المتعلقة بفوائد البلد، حيث تعد ماليزيا في خضم عصر العلوم والتكنولوجيا. وتم اختيار الكلمات مثل الأجهزة والمرافق والأمن والقوات العسكرية وغيرها ككلمات رئيسية تم تطبيقها في هذا البحث. يهدف هذا البحث لتحديد مستوى النظر في أمن المعلومات في ممارسة ظاهرة إحضار جهازك الخاص BYOD في المؤسسة، ثم التعرف على العوامل التي يجب أخذها في الاعتبار لضمان تأمين معلومات المؤسسة مع التمكين في الوقت نفسه من استخدام هذه التقنية BYOD والتأكيد على المخاطر الأمنية التي يمكن أن تكون مرتبطة باستخدامها. تم احصاء 200 مشارك في هذا البحث من القوات العسكرية التي تعمل في الجيش الماليزي من بين أفراد MK PMBTD. كما تم استخدم طريقة البحث الكمي والنوعي باستخدام برنامج SPSS 25.0 للحصول على البيانات من المشاركين. حيث اظهرت نتائج هذه الدراسة أن اعتبارات أمن المعلومات معتدلة وهامة مع نجاح ممارسة BYOD (r = 0.606، p = 0.000) وأيضا تم تنفيذ التدبير الأمني (r = 0.711، p = 0.000) بقوة واهتمام مع نجاح ممارسة BYOD.كما أظهرت المخاطر الأمنية بقوة وكثرة (R = 0,720، p = 0,000) مع نجاح ممارسة BYOD. وكذلك كان معامل بيتا 0.569 وهو أكبر قدر من الرضا عن مخاطر الأمان وهذا يتوافق مع أعلى إحصاء t وهو 8.036. كما يوفر هذا البحث إرشادات تحليلية جيدة بشأن الإطار المفاهيمي لعمل صيانة الأمان من أجل تنفيذ BYOD من

خلال تعزيز إدارة أمن تكنولوجيا المعلومات. كما أظهر البحث أنه من الممكن إنشاء نموذج أمني مناسب لتكنولوجيا المعلومات من أجل تعزيز إدارة الأمن لخاصية إحضار جهازك الخاص او استخدام جهازك الشخصي في العمل (BYOD). ومن ثم، فإنه من خلال هذا النهج المفيد، سيصبح وسيلة فعالة لتحديد العوامل التي تؤثر على كفاءة وفعالية ممارسة إحضار جهازك الخاص او استخدام جهازك الشخصي في العمل ..(BYOD)

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Protective Security Management.

…….
Lili Marziana Bt. Abdullah
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Protective Security Management.

…….
Lili Marziana Bt. Abdullah
Examiner

…….
Muhamad Sadry Abu Seman
Examiner

This dissertation was submitted to the Department of Centre for IT Advancement and is accepted as a fulfilment of the requirement for the degree of Master of Protective Management.

……

Madihah Sheikh Abdul aziz
Head, Department of Centre for IT Advancement

This dissertation was submitted to the Kulliyyah of Information and Communication Technology and is accepted as a fulfillment of the requirement for the degree of Master of Protective Security Management.

…….
Abd Rahman Ahlan
Dean, Kulliyyah of Information and Communication Technology

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Fikri Hanis Bin Md Badarudin

Signature…… Date……30 SEP 2022….

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

BRING-YOUR-OWN DEVICE(BYOD) GUIDANCE: INFORMATION SECURITY CONSIDERATIONS AND RECOMMENDATIONS FOR MALAYSIAN ARMY IN PENINSULAR MALAYSIA

I declare that the copyright holder of this thesis/dissertation are jointly owned by the student and IIUM.

Copyright © 2022 Fikri Hanis Bin Md Badarudin and International Islamic University Malaysia. All rights reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may only be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purpose.

3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Fikri Hanis Bin Md Badarudin

…… ……30 SEP 2022…..

Signature Date

This thesis is dedicated to my late parents for laying the foundation of what I turned out to be in life.

ACKNOWLEDGEMENTS

All glory is due to Allah, the Almighty, whose Grace and Mercies have been with me throughout the duration of my programme. Although, it has been tasking, His Mercies and Blessings on me ease the herculean task of completing this dissertation.

I am most indebted to by supervisor, Dr. Lili Marziana Abdullah, whose enduring disposition, kindness, promptitude, thoroughness and friendship have facilitated the successful completion of my work. I put on record and appreciate her detailed comments, useful suggestions and inspiring queries which have considerably improved this dissertation. Her brilliant grasp of the aim and content of this work led to his insightful comments, suggestions and queries which helped me a great deal. Despite her commitments, she took time to listen and attend to me whenever requested. The moral support she extended to me is in no doubt a boost that helped in building and writing the draft of this research work.

Lastly, my gratitude goes to my beloved wife, lovely children and family; for their prayers, understanding and endurance while away.

Once again, we glorify Allah for His endless mercy on us one of which is enabling us to successfully round off the efforts of writing this thesis. Alhamdulillah

TABLE OF CONTENTS

Abstract……..ii
Abstract in Arabic……..iv
Approval Page……vi
Declaration……viii
Copyright……..….ix
Dedication……..x
Acknowledgements……xi
Table of Contents…….. xii
List of Tables…… xv
List of Figures…… xvii
List of Abbreviation……..xviii

CHAPTER ONE: INTRODUCTION……1
1.1 Background of the Study…… 1
1.2 Problem Statement…….. 2
1.3 Research Question……... 5
1.4 Research Objectives……5
1.5 Scope and Limitation……... 6
1.6 Significance of the Study…… 6
1.7 Organisation of the Chapter…… 7

CHAPTER TWO: LITERATURE REVIEW……..…… 9
2.1 Introduction…… 9
2.2 Bring Your Own Device (BYOD)…….. 9
2.3 BYOD Approaches……..12
2.4 Security and BYOD……13
2.4.1 The Level of Security in BYOD……... 14
2.4.2 BYOD Information Security……17
2.4.3 Security Models for Managing BYOD……19
2.5 BYOD Advantages…….. 20
2.6 Risks in BYOD…… 21
2.6.1 BYOD Disadvantages……...21
2.6.2 BYOD Threats and Attacks…….. 23
2.7 BYOD Vulnerabilities…… 28
2.7.1 Confidentiality…….. 30
2.7.2 Isolation……30
2.7.3 Compliance……... 31
2.8 Mitigation Measures…… 31
2.8.1 Data Leakage…… 31
2.8.2 Unintentional data disclosure……32
2.8.3 Malware-spyware, surveillance, virus, financial malware……32
2.8.4 Network spoofing…… 32
2.8.5 Network congestion…….. 33
2.9 BYOD Considerations……33

2.9.1 Ask the employees…… 33
2.9.2 Agreements……... 34
2.9.3 Quality Security…… 34
2.10 Chapter Summary…….. 34

CHAPTER THREE: RESEARCH METHODOLOGY…….. 36
3.1 Introduction……..36
3.2 Research Design…….. 36
3.2.1 Quantitative Method…… 37
3.3 Research Instruments……...37
3.3.1 A questionnaire……38
3.4 Population and Sample…… 39
3.4.1 Location of Study……. 40
3.5 Data Collection Strategy…… 40
3.6 Data Analysis Strategy…… 41
3.6.1 Descriptive Analysis…… 41
3.6.2 Correlation Analysis……42
3.6.3 Regression Analysis…… 43
3.7 Conceptual Framework……44
3.8 Summary……..45

CHAPTER FOUR: DATA ANALYSIS…….46
4.1 Introduction…… 46
4.2 Pilot Study……46
4.3 Reliability Data……47
4.4 Normality Test……47
4.5 The Background of Respondents……48
4.6 To Assess the Experience Using BYOD…… 50
4.7 Descriptive Frequency Analysis…… 53
4.7.1 To identify the level of information security consideration on the practice of BYOD in the organization……..……... 53
4.7.2 To determine the security measure implemented in BYOD practice within the organization…… 54
4.7.3 To recognize factors that should be considered in ensuring organization's information is secured while enabling the use of BYOD…… 56
4.7.4 To identify the security risk associated with BYOD implementation within the organization…… 57
4.8 The Correlation Analysis……58
4.9 The Regression Analysis……..59
4.10 Summary ……60

CHAPTER FIVE: DISCUSSION, SUMMARY AND RECOMMENDATION……...62
5.1 Introduction……..62
5.2 Discussion……63
5.2.1 The experience using BYOD among Malaysian Army in Peninsular Malaysia……...63

5.2.2 The Level of Information Security Consideration on the Practice of BYOD……64
5.2.3 The security measure implemented in BYOD practice…… 64
5.2.4 The factors that should be considered in ensuring organization's information is secured……66
5.2.5 The security risk associated with BYOD implementation……67
5.3 Limitation of Study……..67
5.4 Direction for Future Research……..68
5.5 Recommendations……68
5.6 Implication……... 69
5.7 Conclusion……... 69

REFERENCES……72

APPENDIXES……... 76

LIST OF TABLES

Table 2.1	BYOD security controls and measures used by the organizations	18
Table 2.2	Threats and Attacks on Mobile Device (Wang, 2012)	29
Table 3.1	Likert's Scale	38
Table 3.2	Level of Variables	42
Table 3.3	Guildford's Rule of Thumb	43
Table 3.4	Criteria of Linear Regression Coefficient	44
Table 4.1	Reliability of Data	47
Table 4.2	Test of Normality for Each Factor	48
Table 4.3	Distribution of Background Respondent	49
Table 4.4	Distribution of Experience Using BYOD	52
Table 4.5	Distribution of Level of Information Security Consideration on the practice of BYOD in the organization	53
Table 4.6	Distribution of Security Measure Implemented in BYOD practice	55
Table 4.7	Distribution of Factors that Influence Efficiency and Effectiveness of BYOD practice	56
Table 4.8	Distribution of security risk associated with BYOD implementation	58
Table 4.9	Correlation between variables	59
Table 4.10	Regression Analysis	60

LIST OF FIGURES

Figure 1.1	Example of the risks of using BYOD in daily life. (Source: Businesswire, 2016)	4
Figure 2.1	The use of password in BYOD	16
Figure 3.1	The conceptual Framework of The Study	44

LIST OF ABBREVIATION

BYOD	Bring Your Own Device
BYOP	Bring your own phone
BYOPC	Bring your own Personal Computer
CIA	Confidentially, Integrity & Availability
CYOD	Choose your own device
HYOD	Here is your own device
MAF	Malaysian Armed Forces
MAM	Mobile application management
MDM	Mobile Device Management
MIM	Mobile Information Management
MVM	Mobile Virtual Machines
OYOD	On your own device

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Military force is one of the most important parties which ensure the security and safety of the people in one country. Malaysia is a country with multiple races which always strongly in its effort to defend the country from any threats and attacks from within or outsiders. Since the age of Independence Day, Malaysia endeavor with many ways in order to preserve the harmonious within the society and within the country. Hence, the military forces become one of the most important shield team for the country from any danger and attack.

Historically, there are many wars before the Independence Day, in a way that many outsiders and foreign countries especially from the high-power invaders such as British, Dutch, Portuguese and Japan. British had interrupted in almost all matters and business within the country except for the royal-king and the custom and religion of the people especially Malays population. Besides, British and all other colonials including Japan had control almost all sources of country's economic, politic and social such as conquered all land resources and taxes as well as placed their representative in the administration of the politic of almost all the states in the country.

In fact, all these colonialism and interruption from other countries can be taken as a lesson for all Malaysians regardless their status and parties to defend the country, to maintain the harmony and to preserve the peace of all individuals in the society. Primarily, these acts of defending, maintaining and preserving the peace and harmony in the country is so much related to the whole concept of the security of the country.

The security is the most noticeable aspect that needs to be strengthened by a state for its own national interest. It does not only refer to military task forces, but also encompasses other sectors including political, societal, economic and environmental security. The security of the state also refers to a variety of continuous activities comprising all aspects of domestic, foreign and security policies. On one hand, it takes bearing from a country's threats and capabilities from the global or international scope or views.

The introduction of security controls on employee-owned device has the potential to compromise employee privacy (Absalom, 2012). Employees may be worried about being monitored and that private data on their portable devices, such as emails, images, and GPS data, may be revealed to their employers. (Lebek et al., 2013). The issues of BYOD and its security has received significant attention; thus, the research is being conducted in order to investigate the use of application of the new and trendy devices which can contributes to as many information, knowledges and connections as the All-in-One concept with the whole countries in the world.

Then, **BRING-YOUR-OWN DEVICE(BYOD) GUIDANCE: INFORMATION SECURITY CONSIDERATIONS AND RECOMMENDATIONS FOR MALAYSIAN ARMY IN PENINSULAR MALAYSIA** is the title that has been chosen for the research upon all the need and relevancies of the security information and knowledges for the benefits of the country, Malaysia in the midst of sciences and technology era. The key words applied in the research such as devices, facilities, security, military forces, etc.

1.2 PROBLEM STATEMENT

Bring Your Own Device (BYOD) is a relatively new phenomenon in which employees connect their personal portable devices to an enterprise network to gain access to corporate information and conduct daily business functions (Miller et al., 2012). The use of BYOD would present a specific issue for protection and privacy. BYOD exposes

companies and organizations to additional security and information privacy risks because it increases the likelihood of sensitive information being exposed to unauthorized entities or persons. As mentioned by Vorakulpipat et al., (2017) that there are many organizations in today's world permit their employees to bring own electronic gadgets such as smartphones or tablets to work and access the corporate network, which is known as bring your own device (BYOD).

To practice, all systems in the country are working with BYOD such as in education, in economic and businesses, in social welfare practices and in the military forces task also. It appears that BYOD enables users to take part more in participate in more work-related tasks by using any endpoint devices and mobile phones, regardless of location or time. Thus, BYOD has provided substantial benefits and convenience to all business activities in all organizations to function efficiently and flexibly (B. Morrow, 2012). As a result, BYOD saves money for businesses because it eliminates the need for employer to provide any devices for their workers.

However, allowing employees to access company information on their own devices raises a number of questions that a company must address in order to meet its information security obligations. There are numerous threats and risks may be faced by all person especially those who work in the field of safety and security of the country such as shown in the figure 1.1 below.

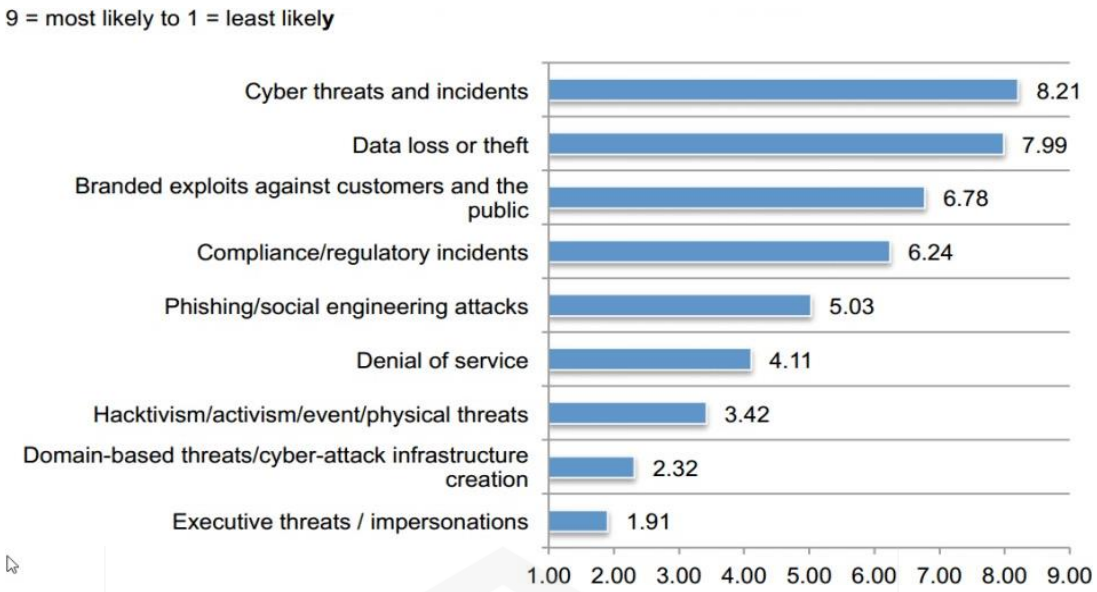

Figure 1.1 Example of the risks of using BYOD in daily life.
(Source: Businesswire, 2016)

According to Drury et.al. (2012), BYOD is commonly used in most countries such as Spain, Brazil, Malaysia and Singapore, the usage of BYOD by organizations are up to 80%, nevertheless the number of employees who obey the policies needed to secure BYOD is extremely low. Subsequently, VMware Asia Pacific (2013) reports that more than 85% of Malaysians utilize their personal computing equipment in the workplace but only 26% are given the support they needed from IT departments.

On the other hand, Juniper Networks (2012) states that global security state of portable devices, services and networks is at a critical state. Most of the advantages of having a BYOD strategy may be lost if security solutions are not put in place (M. Eslahi, 2012). Therefore, it is crucial for organizations especially those who are fully responsible with the safety and security of the people and the country to employ a proper security model for portable devices as the widespread use of portable devices increases the incidence of critical security problems in organizations (J. Lee, 2013).

Apparently, the use of BYOD has recently risen however the numbers of associated studies of its security are relatively low. Security is deemed to be main key issues when considering about BYOD (Miller, Voas & Hurlburt, 2012). Therefore, this

dissertation will focus on investigating information security considerations in BYOD practice in an organization.

1.3 RESEARCH QUESTION

This study will investigate the security of the information on BYOD phenomenon. The investigation is focusing on work environment, with the goal to develop a set of the factors for consideration when developing BYOD.

The present study, within the context of a work environment, will be concerned with the following research questions:

1. What is the level of information security consideration in the practice of BYOD in the organization?
2. What are the security risks related to the use of BYOD in organizations?
3. What are the factors that should be considered in ensuring organization's information is secured while enabling the use of BYOD?

1.4 RESEARCH OBJECTIVES

1. To identify the level of information security consideration on the practice of BYOD in the organization.
2. To identify the security risks which can be related to the use of BYOD in organizations.
3. To determine factors that should be considered in ensuring organization's information is secured while enabling the use of BYOD.

1.5 SCOPE AND LIMITATION

The research will only cover the exploration the scope of the use of BYOD among the military forces in term of factors and its risks, not discussing any other items such as an environmental factor will not be investigated in the study. Then, there are several respondents among the Malaysian Army or soldiers have been involved in this study that has been randomly selected, and not referring to any other group of respondents in the government sectors. The respondent will be among the military forces who work in Malaysian Army, and not referring to any other group of military forces like Navy and Air forces in the country.

This study focused on the factors or conditions which are being considered in using or applying BYOD and its risks as a relation to the security information threats occurrence, not represent any other item or variables. Literature finding will be based on factors or conditions of the consideration of using BYOD and its relation to the information systems. The information systems in other e- government application will not be considered and not be represented by the literature reviews within this study.

1.6 SIGNIFICANCE OF THE STUDY

By conducting this dissertation, consideration of BYOD guidance in information security can be studied. With the understanding of the main risks of BYOD when considering on portable device program, the researchers may propose potential steps to address these risks based on organization's current and most urgent challenges.

This study is about the Malaysian's safety and security in the work environment which have evolved based on situations especially during this modern and global time and why the overuse of BYOD may become a threat to the internal securities. The factors and causes discussed reflect the approach and changes made by government especially among the Malaysian army or soldiers to tackle each issue.

This study is significant since it can help the staffs in the ministry of defends and the soldiers themselves to understand the real phenomena of the security within or outside of the country as well as the current issues such as publics' respond towards the government's acts. By knowing and aware of all happens, they can prepare for any consequences ahead. Additionally, it can upsurge the patriotic spirits among the government members and all the public servants to looking seriously at the importance of the relation between BYOD and the national security of the country each time in present and in the future. By comprehending the importance of both variables, all members of the country will be hand in hand to make sure the harmonious life of the people. It will be an interesting starting point for more research related to this field.

In spite the high focus on the factors and the suitable conditions for the use of BYOD, there is still lack of understanding concerning the potential impacts of the misused or leaking of the information along the application of BYOD within the organizations. Thus, this study is significance for all members of the government and the publics, not only to military forces, to identify the safety and security guaranteeing of the using of BYOD in their work life. So, it can help creating the greater awareness among all individuals in the country about the importance of the internal security especially in term of information security.

For academic perspectives, this study also significance in providing new information to the policy makers, the government, the academic researchers and other decision makers. In order to help them organizing their understanding about the importance of the correct and proper use of BYOD and the risks of it may exist towards the national security.

1.7 ORGANISATION OF THE CHAPTER

Chapter One point up the whole sketch of this research. As well as introducing the background of this research, problem statement, research questions, research objective, significance of study and the scope of study are also adopted to direct the next chapters.

Chapter Two highlighting in reviewing literature and prior studies which connected to each independent and dependent variable, conceptual frameworks in this research. The researcher will explore the previous studies and journals regarding the concept of BYOD, the importance BYOD in the relation with the information security systems, and BYOD advantages and disadvantages. Theories and models related to the use of BYOD and the national security of the country.

Chapter Three describes on research methodology encompassing research design, sampling techniques, data collection method, research instruments, variables and constructs measurement, data processing and analysis techniques.

Chapter Four demonstrates the pattern of results through statistical techniques such as SPSS analyses. The results analyses are consequently validated against research questions developed in previous chapters.

Chapter Five will summarize all analysis and discussion on major finding. As well, this chapter concludes conclusion, implication and research limitations. Limitations of this research and recommendations for future research will be elaborated in this chapter.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

Chapter 2 has a task to review and gives a deeper understanding to the reader on the concept of BYOD, the importance BYOD in the relation with the information security systems, and BYOD advantages and disadvantages. The issues related to the use of BYOD and the national security of the country especially that related to the information security.

2.2 BRING YOUR OWN DEVICE (BYOD)

Bring your own device (BYOD) also called bring your own technology or tube (BYOT was invented by Ryan Zetterberg on April 4 2016, in which it asks to bring your own phone (BYOP). Moreover, bring your own Personal Computer (BYOPC) refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets and smart phones) to their workplace. Those devices are used to access privileged company information and applications Tony Bradley (2011). It is relatively new paradigm in tele-commuting purposes. According to Boon & Sulaiman (2015), BYOD is a practice that has been embraced by most businesses and organizations, estimating that 200 million out of 360 million users use their personal devices for work-related activities because can give job satisfaction as it produces an improvement in productivity. This is supported by Page (2013) who shows that 80% of the companies and organization who allows a BYOD program have seen a rise in productivity. In other way, the companies and organization don’t have to cope with the devices or data plan’s