DATA LEAKAGE MODEL IN THE USE OF SOCIAL MEDIA AMONG MALAYSIAN ARMED FORCES PERSONNEL

NUR ALFA MAZLIN BINTI MASDAN

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : Nur Alfa Mazlin binti Masdan

Date of birth : 28 July 1981

Title : Data Leakage Model In The Use of Social Media Among Malaysian Armed Forces Personnel

Academic Session : 2016/2017 Semester 1

I declare that this thesis is classified as :

☐	**CONFIDENTIAL**	(Contains confidential information under the Official Secret Act 1972)*
☐	**RESTRICTED**	(Contains restricted information as specified by the organization where research was done)*
√	**OPEN ACCESS**	I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

SIGNATURE	**SIGNATURE OF SUPERVISOR**
810728-05-5368 (T3008509)	**DR. NOR ZAIRAH BINTI AB RAHMAN**
(NEW IC NO./PASSPORT)	**NAME OF SUPERVISOR**
Date : 30 DECEMBER 2016	Date : 30 DECEMBER 2016

NOTES : * If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Science (Information Assurance)"

Signature	: …….....
Name of Supervisor	: Dr. Nor Zairah binti Ab Rahim
Date	: 30 December 2016

DATA LEAKAGE MODEL IN THE USE OF SOCIAL MEDIA AMONG MALAYSIAN ARMED FORCES PERSONNEL

NUR ALFA MAZLIN BINTI MASDAN

A project report submitted in partial fulfilment of the requirement for the award of degree of Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

DECEMBER 2016

DECLARATION

I declare that this research entitled ***"Data Leakage Model In The Use of Social Media Among Malaysian Armed Forces Personnel"*** is the result of my own research except as cited in the references. The research has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signature : ……

Name : NUR ALFA MAZLIN BINTI MASDAN

Date : December 2016

DEDICATION

Specially dedicated to my family.
Thank you so much for all of your strong support, endless love, trust, constant encouragement over the years, and a prayer throughout my studies.

ACKNOWLEDGEMENT

Alhamdulillah,

I wish to express my sincere appreciation to my honorable supervisor, Associate Professor Dr. Zuraini Ismail and Dr Nor Zairah binti Ab Rahim for her endeavor approach, outstanding supervision, valuable support and sincere guidance by which it has been possible for me to complete this research project.

My heartfelt gratitude also goes to my beloved family and friends, thank you for the encouragement, support for being my inspiration, for your understanding and for your endless love.

ABSTRACT

Freedom of access in the social media has raised the profound effect on confidential data dissemination and its security. The scarcity of security awareness particularly in Malaysian Armed Forces personnel practices in handling confidential data remain of utmost. Along with the subversion threats involving the Malaysian Armed Forces personnel with the rise of Islamist militant group of Islamic State where the cyber platform is used to spread the idealism as the modus operandi. This research aims to identify factors influencing data leakage attributes in the use of social media for the Armed Forces. This is executed by designing data leakage model and evaluating the proposed model. A quantitative research methodology is employed whereby, 187 questionnaires were distributed to personnel in the Malaysian Armed Forces from Prebat to Major rank. 100% responses rate was recorded. SPSS version 19 is used for analysis. The results revealed significant with strong positive correlation between the identified attributes, namely computer usage behavior, security education and knowledge, security awareness and policy acceptance and understanding are influencing the received control data leakage. This research may assist the Armed Forces in secured practices acquired in handling organisation's valuable assets which requires special guardianship on its perseverance.

ABSTRAK

Kebebasan akses menggunakan media siber telah menyumbang kepada kesan yang mendalam terhadap penyebaran maklumat terperingkat dan keselamatan. Kekurangan kesedaran etika teknologi terutamanya di kalangan anggota Angkatan Tentera Malaysia dalam mengendalikan maklumat terperingkat menjadi perhatian utama. Akibat daripada ancaman subversif yang melibatkan anggota dengan kebangkitan kumpulan militan Islam, "Islamic State" menggunakan modus opendi media siber untuk menyebarkan idealisme. Kajian ini bertujuan untuk mengenalpasti factor-faktor penyumbang kepada ketirisan data melalui media siber dikalangan nggota Angkatan Tentera Malaysia dalam pengendalian maklumat terperingkat. Ini dilaksanakan dengan merekabentuk dan menilai model factor ketirisan data yang dicadangkan. Kaedah penyelidikan kuantitatif dijalankan di mana 187 soal selidik telah diedarkan kepada anggota di dalam Angkatan Tentera Malaysia berpangkat Prebat ke Mejar. 100% kadar maklumbalas direkodkan. SPSS versi 19 digunakan untuk analisis. Hasil kajian menunjukkan signifikan dengan korelasi positif kukuh antara ciri-ciri faktor kesedaran keselamatan data di kalangan pekerja, kelakuan pengguna semasa menggunakan peralatan komputer, pengetahuan berkenaan keselamatan data dan penguatkuasaan polisi di dalam organisasi. Kajian ini dapat membantu Angkatan Tentera dalam amalan terbaik dalam memastikan kelangsungan dalam mengendalikan asset organisasi yang bernilai yang memerlukan penjagaan rapi.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xv
	LIST OF ABBREVIATIONS	xvii
	LIST OF APPENDICES	xviii
1	**INTRODUCTION**	**1**
	1.1 Overview	1
	1.2 Background of The Problem	3
	1.3 Problem Statement	8
	1.4 Research Question	9
	1.5 Research Objectives	9
	1.6 Research Aim	10
	1.7 Research Scope	10
	1.8 Significance of the Research	10
	1.8.1 Methodological Contribution	11
	1.8.2 Theoretical Contribution	11
	1.8.3 Practical Contribution	11

1.9 Organisation of the Thesis 12
1.10 Summary 13

2 LITERATURE REVIEW 14
2.1 Introduction 14
2.2 Data Leakage 15
2.2.1 Data Leakage Vector 16
2.2.2 MAF in Data Handling Isues 18
2.3 Human Factor in Information Security 21
2.4 Common Behaviors Resulting in Potential Risk of Data Leakage 25
2.5 Security Awareness 27
2.5.1 A Framework of Security Awareness and Information Security 28
2.6 Data Leakage in The Use of Social Media Attributes From Structured Literature Review 34
2.6.1 SLR Review Method 35
2.6.2 Selection of Related Studies 41
2.6.3 Review Outcome 42
2.6.4 Synthesizing of the Evidence 43
2.7 Summary of Related Variable 44
2.8 Proposed Conseptual Model for Factors of Data Leakage in The Use of Social Media in MAF 45
2.9 Summary 46

3 METHODOLOGY 47
3.1 Introduction 47
3.2 Research Procedure 47
3.3 Phase 1: Information Gathering and Project Planning 48
3.3.1 Preliminary Investigation 49
3.3.2 Structured Literature Review 52
3.4 Phase 2: Design 53
3.4.1 Chosen Methodology 53
3.4.2 Questionaire Design 54

	3.5 Phase 3: Implementation	55
	3.5.1 Research Population and Sample	55
	3.5.2 Pilot Study	56
	3.5.3 Actual Survey	57
	3.6 Phase 4: Analysis	58
	3.7 Phase 5: Report Writing	58
	3.8 Research Deliverable	58
	3.9 Summary	60
4	**FINDING AND ANALYSIS**	**61**
	4.1 Introduction	61
	4.2 Reliability	61
	4.3 Face Validity	62
	4.4 Normality Test	63
	4.5 Descriptive Statistics	64
	4.5.1 Respondent Demographic	64
	4.5.2 To Identify The Data Leakage Attributes	67
	4.5.2.1 Computer Usage Behavior	67
	4.5.2.2 Security Awareness	68
	4.5.2.3 Policy Aceptance and Understanding	69
	4.5.2.4 Security Education and Knowledge	70
	4.5.3 To Identify The Most Data Leakage Attributes	71
	4.5.4 To Describe The Data Leakage Factors	72
	4.6 Statistical Test	73
	4.6.1 Correlation	73
	4.7 Conclusion	77
5	**DISCUSSION AND CONCLUSION**	**78**
	5.1 Introduction	78
	5.2 Summary of the Research Finding	78
	5.2.1 Findings for First Objective	79
	5.2.2 Findings for Second Objective	79
	5.2.3 Findings for Third Objective	80

5.3 Recommendations 82
5.4 Limitation of the Research 83
5.5 Recommendation For Future Research 84
5.6 Research Contribution 85
5.6.1 Theoretical Contribution 85
5.6.2 Methodological Contribution 86
5.6.3 Practical Contribution 86
5.6 Conclusion 86

REFERENCES **88**
Appendices A-C 91-97

LIST OF TABLES

TABLE NO.	TITLE	PAGE
1.1	Statistics of electronic information leaks in the government sector in 2012 (MAMPU, 2013)	4
2.1	Common unintentional data loss theme (Young, 2011)	27
2.2	PICOC structure of research question	37
2.3	Synonyms and alternatives	38
2.4	Concatenation of alternative words with boolean or	38
2.5	Initial databases primary searches string results	39
2.6	Final articles selection	40
2.7	Article searches breakdown	42
2.8	Evidence synthesising findings	43
2.9	Related research on data leakage prevention	44
3.1	Interviewees' profiles for preliminary investigation	50
3.2	Proposed conceptual model for factors influencing data leakage in the use of social media	55
3.3	Population size of selected maf personnel categorised by rank	56
3.4	Population size of actual survey distribution	57
3.5	Summary of research deliverable	59
4.1	Test of reliability	62
4.2	Test of normality for each factor	63
4.3	Number of respondents based on gender	64
4.4	Number of respondents based on service rank	64
4.5	Number of respondents based on experience.	65
4.6	Number of respondents based on education level	66
4.7	Number of respondents based on sharing confidential	

	information	67
4.8	Number of respondents based on updating status using social media	67
4.9	Frequencies and percentages of computer usage behavior	68
4.10	Frequencies and percentages of security awareness	69
4.11	Frequencies and percentages of policy acceptance and understanding	70
4.12	Frequencies and percentages of security education and knowledge	71
4.13	Rank of factor	72
4.14	Frequencies and percentages of data leakage factors	73
4.15	The relationship behavior of computer use and factors of data leakage	75
4.16	The relationship the education security and knowledge and factors of data leakage	75
4.17	The relationship the security awareness and factors of data leakage	76
4.18	The relationship the relationship with policy acceptance and understanding and factors of data leakage	76

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	Literature review map	15
2.2	Aspects on information security (Lean-ping & Chien-fatt, 2014)	21
2.3	Security framework (Marko Van Zwam, Martijn Knulman, 2012)	22
2.4	DLP conceptual model (Young, 2011)	23
2.5	Framework of IT governance effectiveness (Mohamed & Singh, 2012)	24
2.6	Model of managerial effectiveness in information security (Knapp, 2005)	29
2.7	Means-ends objectives network for ICT security awareness (Kruger HA, L Drevin & Science, 2007)	30
2.8	Framework for monitoring internal threats to security data (Yayla, 2011)	31
2.9	Framework for implementation issues safety awareness program (Martinez et al., 2010)	31
2.10	Factors for implementing and adopting IS culture and practices in Saudi Arabia (Alnatheer & Nelson, 2009)	32
2.11	Conceptual information security framework for higher education institutions (HEIs) (Ismail et al., 2010)	33
2.12	Model for factor influencing information security factor (Hassan &Ismail, 2012)	34
2.13	Phases and stages of systematic literature review	36
2.14	Skeleton of conceptual model for data leakage factors	37
2.15	Identifying relevant literature	42

2.16	Proposed conceptual model data leakage model in the use of social media for MAF	45
3.1	Research procedure	48
5.1	Summarizes the relationships between all variables	81

LIST OF ABBREVIATIONS

AFGI	-	Armed Forces General Instruction
CO	-	Commanding Officer
DISD	-	Defence Intelligence Staff Division
IS	-	Islamic State
IV	-	Independent Variable
DV	-	Dependent Variable
MAF	-	Malaysian Armed Forces
NCO	-	Non Commission Officers
PICOC	-	Population, Intervention, Comparison, Outcomes and Context
SLR	-	Systematic Literature Review
MAMPU	-	National Security Council
ROC	-	Royal Ordnance Corp
FTP	-	File Transfer Protocol
DLP	-	Data Leakage Prevention
ICT	-	Information And Communications Technology
HEI	-	Higher Education Instituition
IPVPN	-	Internet Protocol Virtual Private
DEMS	-	Defence Electronic Messaging System
C2	-	Command and Control
SETA	-	Security Education Training and Awareness

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Interview Outline	91
B	Revised Questionnaire Structure	92
C	Example of case: Army Cyber Monitoring Team System – List of Monitoring	96

CHAPTER 1

INTRODUCTION

1.1 Overview

Information security plays an important role in ensuring that all information is protected. Safety information is also referred as computer security is defined as the protection granted to automated information systems to achieve the objective to maintain the confidentiality, integrity and availability resource information systems (Zafar, 2013). In other definitions, synonyms data leaks with a leak of information from the illegal transmission of information within an organization for destinations outside or receiver. Unauthorized transmission does not automatically mean an accidental or malicious (Institute, 2007).

Social media is the computer-mediated tools that allow people to create, share or exchange information, ideas, images or videos in virtual communities and networks. Social media is defined as a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content (Andreas, Haenlein, 2010). Furthermore, social media rely on mobile technology and web-based platform for creating highly interactive environment where individuals and community's stock, make friends, discuss, and modify user generated content. They introduce major changes and extensive communication between businesses, organizations, communities and individuals (H. Kietzmann, Jan; Kristopher Hermkens, 2011). Social media has become one of the internet's most popular services in the world such as Facebook and MySpace. Until 2015, Alexa, a company that tracks web traffic, ranking these sites as two sites most visited in the world, where Facebook is

the second for both Google's and the US ranking (Alexa, 2014). Facebook is one of the web's most popular social network, today has reached a membership of over 900 million, followed by Twitter has reached 310 million members and LinkedIn has reached a membership of more than 255 million members by rank eBizMBA a company that also tracks web traffic (eBizMBA, 2015).

The popularity of social media and it is use increasing in the workplace provides some anxiety for employees to maintain a safe environment for storing and distribution of information. A statistic shows in Shanghai Globe GO Web design Company estimated penetration of social media in the Asia Pacific region sits at 25% at the moment is an impressive figure, especially when it is about the fact that the Asia-Pacific region accounted for 52.2% of the social global media users. 97.3% of active social media users in the Asia Pacific region to access social media on their mobile devices. Asia is important to the growth of Facebook, in view of the area has 426 million monthly active users. It also shows that Malaysia is the third country in Asia has spent 3.3 hours per day for social media after the Philippines and Thailand (GO Globe, 2015). Industry Performance Report 2013 Report, published by Internet regulator, the Malaysian Communications and Multimedia Commission (MCMC) showed 19.2 million Internet users in Malaysia, 15.6 million of whom are active on Facebook, (MCMC, 2013).

Social media mistakes by members of the Armed Forces have been at risk of compromising the operation and security of the nation by leaking the patrol, sensitive details of the visit and photograph the restricted area (Ben Farmer, 2014). The Telegraph reported on 6 July 2014 that there were some high-profile cases Military defense leaked confidential and sensitive information via social media. In 2013, soldiers who had signs of past military patrol in Afghanistan on Twitter. In another, the details of the movement of forces and closing bases in Afghanistan have been shared on Facebook (Ben Farmer, 2014). The cases illustrate the dangers arising from the military widespread use of social media such as Twitter and Facebook. Therefore, it is very important to maintain a safe environment for maintaining and distributing data from leaking.

1.2 Background of the Problem

Irresponsible use of social media has caused adverse effects to the organization in terms of putting the organization's network and malware risk system, which led to legal action that has the potential for copyright and defamation, loss of productivity, and significantly affect the organization's reputation and future income front (Colwill 2010; Gudaitis, 2010; Young, 2010).

More recently, social media has been the target of cyber criminals not only to steal information, but also to use them for storage and bandwidth capacity botnet command and control (Everett, 2010; Smith & Koppel, 2009; Westervelt, 2009). To make matters worse, Facebook profile is now available for download from the website, torrent disclosing information more than 170 million users worldwide (Paul, 2010).

Moreover, cyber criminals today are more interested in collecting information, the organization, from the famous to take down the network (McAfee, 2010). Some of them are sponsored by certain parties to perform highly complex attack to steal sensitive data from organizations targeted by their employees. They use the information available in the public domain, particularly online social media to gather as much information about key individuals before launching spear-phishing techniques and social engineering to get the credentials to access valuable information (Smith & Koppel, 2009; Sophos, 2010; Symantec, 2015). This cyber espionage booming due to the proliferation of social media.

Thus, both small and large organizations, government agencies or private companies, need to pay close attention to social media usage among their employees. They cannot rely solely on technical controls to combat this problem because it involves human weaknesses that need to be covered by the control behavior change.

In Malaysia, a study from the National Security Council (MAMPU) and the MAMPU concerning electronic data leakage in the government sector for the year 2012 found that almost 50% of the source of leakage is of email (MAMPU, 2013).

Most government departments in putting into their information security policies on the importance of data leakage, but some of them do not implement the solution. The problem is that most users do not realize the impact of the leak. It has been proven by a study conducted by the National Security Council and the MAMPU concerning electronic data leakage in the government sector (MAMPU, 2013). Table 1.1 shows the statistics of electronic data leakage in the government sector for the year 2012.

Table 1.1: Statistics of Electronic Information Leaks in the Government Sector in 2012 (MAMPU, 2013)

Medium / Source	**(%)**
E-mail	50
Laptop Computer	48
Internet	46
USB media	43
Remote Access by Service Provider	42
Smart Phone	41
Desktop Computer	40
External Storage Media	39

The most significant result of the leakage of data, including substantial financial impact due to loss of intellectual property, other than that, information leaks can also cause financial losses, damage to the reputation of the government, remained negative publicity and loss of or damage to sensitive information and damage to the reputation of the government through information disclosure Sensitive to the public or unauthorized recipients (Technology, 2009). It is important

to realize that technology is only as effective as the people and the process behind it. Human error, ignorance, omission, or failure to comply with the policies that are available are most of the time the cause of data breaches and information leaks (Marko and Martijn, 2012).

The incident occurred will damage the shield of confidentiality, integrity and availability of the organization. Usually it is caused by human error and technology. Employees are the key factors that can cause great harm to the confidentiality, integrity, or availability of information through intentional activities. Thus, the behavior of the human factor should be changed to ensure standard practices carried out in handling information assets. The level of awareness among workers should be strengthened within the organization.

From the Malaysian Armed Forces (MAF) aspects, there have been situations that have triggered to the development of technology ethics in handling confidential information. There were initially four main manifestations of threats to the MAF security which as allotted in Secretariat, A. (1985) which are:

i. Subversion where the personal loyalty has diverted.

ii. Espionage by performing clandestine and unlawful act of acquiring information.

iii. Sabotage used by a grudge against authority personnel.

iv. Human failings that lead to security breaches to the unauthorised hands because of negligence to security instruction.

At present, the rise of an Islamist militant group, Islamic State (IS) in Iraq and Syria has struck a significant concern among leaders specifically in MAF which signified the subversion threats involving the MAF. The scenario has been taken earnestly as one of the Parliament's members raise the IS issues in the MAF personnel latest status and level of engagement in IS to the MAF representative, the

Deputy of Defence Minister (The Straits Times, 2015). The issue has uncovered a total of six MAF personnel from tri-services which has been arrested by Bukit Aman's Counter Terrorism Branch on suspicion with IS's involvement.

Thus, it is seen as the deliberate threats in which the modus operandi used the cyber medium to spread the idealism among MAF personnel of the concept of jihad by spreading pictures and videos of Muslims' persecution and murders around the world (Directorate, S., 2015). The concern towards the MAF security threats is reflected in this kind of involvement whereby extremist always tries to widen the chances of new recruitments and MAF personnel are of favor as they were equipped with skills required by the group to expedite its activities unlike civilian that need to be trained. Among them are skills in weapon handling, bomb experts, tactical experts, and doctrine disclosure experts.

These subversive threats scenario of IS could be further lead the MAF personnel to be tackled with sabotage threats by using cyber platform as the medium which might lead the espionage threats from the foreign intelligence organisations to further strengthen their surveillance over MAF security using the information exposure by the irresponsible personnel.

In addition, there were overlying cases of incompliance towards the Armed Forces General Instruction's (2013) (AFGI) (Secretariat, A., 2013) in the Supreme Commander of the Army Chief's meeting chaired by the Army Chief, General Datuk Raja Mohamed Affandi bin Raja Mohamed Noor which was attended by the first eleven senior officers in the Army as well as the representative from Armed Forces Headquarters. In the meeting, the representative from the Army Cyber Monitoring Team has presented several cases involving cyber platform, especially through Facebook and a blog that could lead to the compromised and prejudicial towards the MAF organisation secrecy as a whole.

Reports from the Army Cyber Monitoring Team (2015) indicates that from the randomise checked accounts started from December 2014, there were 2 accounts

which have the elements that contributed to the security issues in the MAF followed by 8 accounts, 5 accounts, 5 accounts, 3 accounts, 3 accounts in January 2015, February 2015, Mac 12015, April 2015 and latest was May 2015. Among them are the Facebook account of the army personnel which comprised the negative elements that broadcasted image of meeting attended, unintended displayed of operations folder, broadcasted image of politics party, broadcasted the superior movement, displayed images of forces readiness, and those categorised as confidential information which opposed to the AFGI clause 29 C (6), broadcasted the image of classified document with confidential information as opposed to AFGI clause 29 C (1), broadcasted images of provocation element as opposed to AFGI clause 29 C (4) and published the statement that rise prejudicial to the MAF, published image in improper attire over clothing, broadcasted images of base location, broadcasted images of Armed Forces barrack, broadcasted video of military training song group, broadcasted images of joining illegal group, broadcasted images of illegal animals hunting as well as pressed 'Like' to most images of unauthorised religious groups and anti-government which contradict to the clause 29 C (8) of AFGI respectively.

Whereas, the blogs identified also by the Army Cyber Monitoring Team (2015) are the army personnel blogger that recounts the origins of the IS establishment without valid evidence and supports others views in favour of IS. The blogger buried the misconception spirit of martyr upon the death of Malaysians that joined IS which is seen as uplifting the MAF personnel based on the crafted storyline and uploading video of IS's martial art training to raise others spirit to join and expressing opinion by supporting the IS idealism. Those are all the cases that require attention to the development of adequate policy and awareness on technology ethics in an effort to have the right behaviour and perception in differentiating personal and sensitive information which are confidential.

Inherited from the Secretariat, A. (1985) of Malaysia Armed Forces Security Instruction and Government Security Instruction, the Armed Forces Security Instruction that will be distributed in the near future has put into realisation such that the available instructions will further be enhanced and customised in accordance with

the present cyber platform technology and threats to be adhered by all MAF personnel.

Seen from the exposure threats of unauthorised access such as hacking, fraud, counterfeiting, interception, data disclosure, and malicious code (Cobb and Lee, 2014) along with Electromagnetic Pulse, Ionising Radiation, Electromagnetic Compatibility and Radio Frequency Interference, threats are all vulnerable to the information technology systems (Hoad and Jones, 2004) which is capable in affecting data confidentiality, integrity and availability. The existence of new methods intrusion into a formidable ICT network has forced all levels of MAF personnel to inculcate ICT security culture in handling the confidential information.

1.3 Problem Statement

Malaysian Armed Forces have increased their use of information technology as their primary task as national security front row with social media practices, employees are exposed to social media in their work. The freedom of access in the cyber platform which resulted from technologies proliferation through mobile network, internet or even static network for instance via smart phone, personal digital assistant, and laptop have subsequently contribute to the profound effect on the confidential information contamination and its security.

Through preliminary interviews, it has been concluded that the MAF is struggling to achieve information superiority title due to the technology advancement. This may be difficult to accomplish as the personal disrespect the handling of data by not taking serious compliances in its preservation. Instead of the effort in prohibiting the threats, exploitation and the outsider intervention, the internal elements of the insider threats is seem to be the largest contributor to the data leakage to the outside world due to the personnel mishandling (Secretariat, A., 2013). There is a need to identify the data leakage in the use of social media in the Malaysian Armed Forces for ensuring that data are secured and protected from

leaks. It is important to study the data leakage in social media usage among members of the MAF.

1.4 Research Questions

Research questions are identified as follows:

i. What are the data leakage in the use of social media among the personnel of the MAF?

ii. How to design the data leakage model in the use of social media for the Armed Forces?

iii. How to evaluate the data leakage model in the use of social media for the Armed Forces?

1.5 Research Objectives

The objectives of this research are:

i. To identify the data leakage in the use of social media among the personnel of the Armed Forces.

ii. To develop a conceptual model of data leakage among the Armed Forces.

iii. To evaluate the data leakage model in the use of social media among the Armed Forces.

1.6 Research Aim

The aim of this research is to identify the data leakage attributes in the use of social media for the MAF, to design and evaluate the data leakage model in the use of social media for the Armed Forces. The tested model serves to assist the MAF's superior in identifying the baseline required for each MAF personnel in practicing the most secured way in handling a data from being leaked along with factors of data leakage attributes found in this research.

1.7 Research Scope

The scope of this research is restricted to data leakage in the use of social media in military organization specify Facebook as a tool had been chosen for social media. The Royal Ordnance Corp (ROC) of the Malaysian Armed Forces is chosen as the unit of analysis which involved Non Commission Officers (NCO) personnel from Prebet to Warrant Officer Class I in rank and Officers from Second Lieutenant to Major in rank. A quantitative method of survey is conducted using self-administered questionnaire. Data collected is analysed using the SPSS Version 19.

1.8 Significance of the Research

The research conducted contribute to the three perspectives which are the methodological, theoretical, as well as, practical perspectives. It is seen as an effort in promoting the factors of data leakage issues of the Armed Forces personnel which are needed in order to handle the confidential data from being leaked. Thus, the sections described the significance of the research from the methodological, theoretical, and practical perspectives respectively.

1.8.1 Methodological Contribution

As there is a lack of study using quantitative analysis on data leakage in military environment, therefore this research attempts to provide more information on factors influencing data leakage in MAF organisation. The survey focuses on military personnel from Prebat to Warrant Officer Class I to Officer's Rank from Second Lieutenant to Major in the selected personnel of the MAF.

1.8.2 Theoretical Contribution

Several models gathered from the theoretical academic standpoint were referred which are among them are the model of antecedent and outcome of Model for Factor Influencing Information Security Factor introduced by Hassan & Ismail. (2012), the model Of Managerial Effectiveness in Information Security introduced by Knapp (2005), Framework for controlling insider threats to information security introduced by Yayla (2011). The model is then consecutively being compared and the relationship is mapped along with attributes found on the Systematic Literature Review (SLR). These steps are achieved by the availabilities of the model presented by previous researches towards the potential identification of the deliverable. Therefore, these model are integrated and tested in a military environment.

1.8.3 Practical Contribution

This research will be served as a direction to the managerial perspective of the Armed Forces organisation in viewing the attributes of data leakage model in the use of social media. With the to-be distributed Armed Forces Security Instruction, the outcome of this research will comprise of the attributes among the selected population that can be further measured to others military organisation in a wider scope. It will help the policy maker to make strategic assumptions towards the

refinement of the MAF personnel in handling the confidential data which are known to be sensitive information from the derived model.

It is furthermore equipped an insight that enables the management to strategically formulate the policies creation, personnel privileges management, planning for better training and awareness program checklist and personnel employment screening including personnel background checks towards instilling a strong security culture in the Armed Forces environment. The contribution would instantaneously impress the strategic managerial to respond with the practical implementation of the betterment of the whereabouts, footing, and setting of the organisation.

1.9 Organisation of the Thesis

This research is formed up in five chapters altogether where the first chapter illustrates the overview, background of the problem, research questions, objectives, scopes and the significance of the research being conducted, followed by the second chapter that literally discussed in the literature review of the embodiment of the title selected to gather the knowledge of the current related research area. It also discussed the proposed model for the factors of data leakage in the use of social media. The third chapter depicts the research methodology that is being followed in order to complete the research works. In this chapter, the research technique and operational framework is being rendered in details with the contemplation to complete the research correspondingly according to the work flow. The fourth chapter discusses on the findings and analysis that have been collected from the questionnaires. The last chapter that is the fifth chapter presents and discuss the conclusion of the research which are the research achievement, challenges, and constraints in conducting the research. Future recommendations together with the summary of the research are also introduced in this chapter.

1.10 Summary

This chapter begins with the overview of the data leakage in the use of social media along with the background of the problem, problem statement, project objectives, project aims, project scope, and significance of the research that comprises of methodological, theoretical as well as practical contributions. Next, the Literature Review chapter will be introduced that involved the background of the research through several readings in the related topics as well as the proposed model.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides an overview of the literature review related to security awareness, human behavior and data leakage prevention. All items will be forming a guideline to identify problem, methodology, framework and model.This chapter has ten sections. The first section is the introduction followed by the second section that reviews of data leakage related studies that consists of definition, data leakage vector and further down on data leakage prevention and related models. Next, the third section discusses the issues in the Armed Forces. The fourth and fifth section depicts the MAF and other organisation confidential data handling respectively. The sixth section discusses the data leakage in use of social media and continues with the seventh section which describes four attributes that affect the data leakage in use of social media resulted from the Systematic Literature Review. The eighth section summarises the related variables followed by the ninth section whereby the proposed conceptual model for the data leakage in use of social media is depicted. Tenth section ends the chapter. Figure 2.1 illustrates the Literature Review Map.

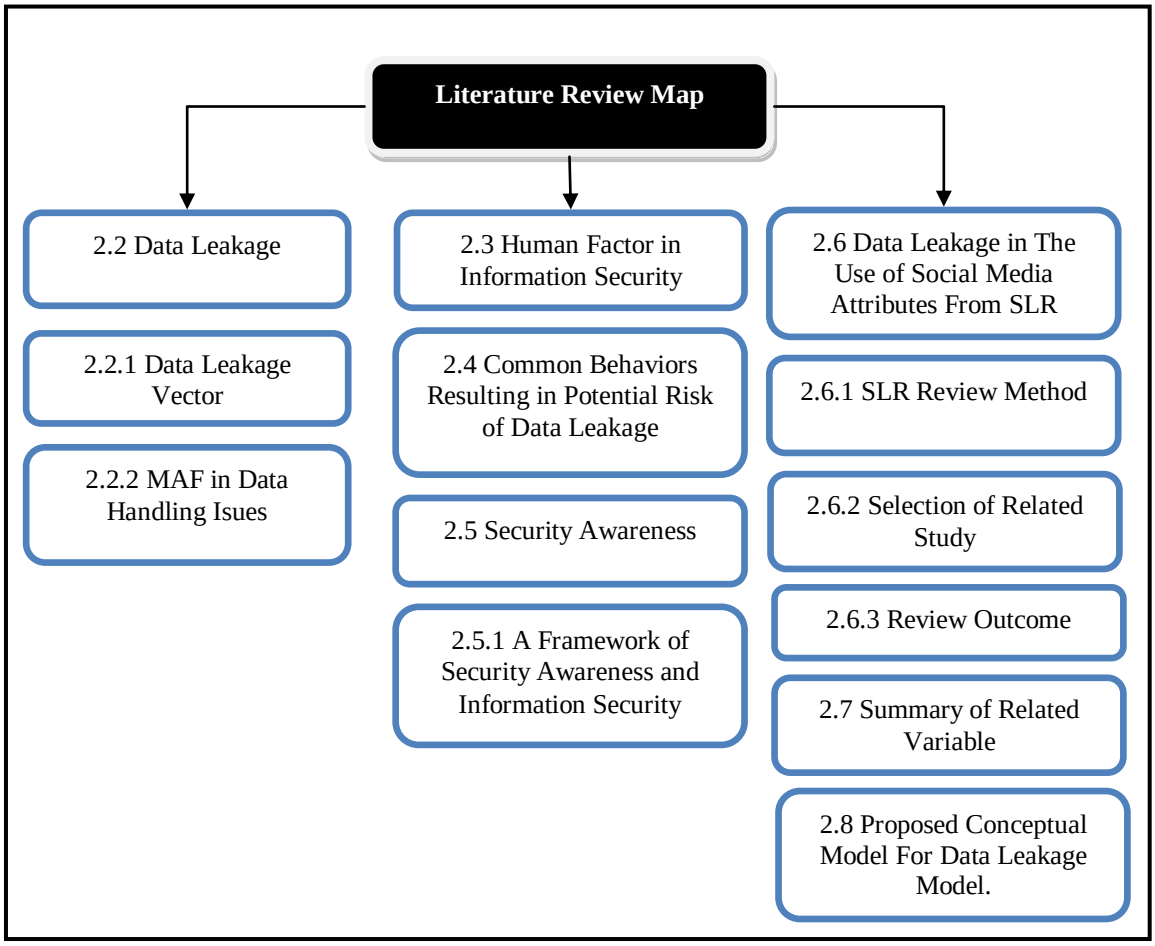


Figure 2.1 Literature Review Map

2.2 Data leakage

Term "leak" by government agencies is the release, unauthorized public information channels of previously undisclosed government in- formation. There are two types of leaks; authorized and unauthorized. (Dw, Zrun, Review, &Katzt, 2012). Data leakage is defined as a breach of the confidentiality of information, typically originating from staff inside an organisation and usually resulting in internal information being disclosed into the public domain (Nuha, Molok, & Ahmad, 2010).

Data leakage also known as information leakage also can be described when sensitive data are revealed intentionally or not intents to unauthorized parties. The information leaked out can either be private in nature and are

deemedconfidential, such as credit card numbers or information that could be used by attackers to further exploit the system (Datardina & Leung, 2009). Although data leakage or unintentional information disclosure can be caused by malicious and non-malicious insiders, non-malicious insiders are the riskiest since accidental security incidents happen more often and have greater potential for harm than malicious insider attacks (Nuha et al., 2010). This is because non-malicious insider could hardly be expected based on their everyday behavior. They are considered harmless because not indicate any potential to be a source of threat to the organization.

Data leakage threat has become an important matter in informationsecurity research, especially data leakage caused by insider, which has seriously affected the security organizational property and personal privacy. In present authorized insider lack necessary restraint devices, and existing research on insider threat mainly focuses on theoretical sensing or detecting analysis phase without practical security awareness. Traditional data leakage prevention technologies are mainly based on domain, which is partitioned into different security domains according to data protection requirements and limits the data flow between security domains through firewall, encryption and terminal control (Wu et al., 2011).

In this previous research, they aimed at data leakage caused by insider istaken into the data leakage threat, active prevention. They propose an active data leakage prevention model. By adding a secure data container to execute security prevention mechanism, the model can ensure that data is used in a reliable and controllable environment.

2.2.1Data leakage Vector

There are numerous ways sensitive data can be revealed to untrusted third parties (Raman, Kayacık, & Somayaji, 2011). Transmission through all other possible channels being recognized in order to prevent data leakage (TrendMicro, 2012). According to data compiled from EPIC.org and PerkinsCoie.com, 52% of

Data Security breaches are from internal sources compared to the remaining 48% by external hackers in a 2010. The noteworthy aspect of these figures is that, when the internal breaches are examined, the percentage due to malicious intent is remarkably low, at less than 1%. The corollary of this is that the level of inadvertent data breach is significant (96%). This is further deconstructed to 46% being due to employee oversight, and 50% due to poor business process (Institute, 2007). SANs Institute in their research named list of potential data leakage vector as below:

i. Instant Messaging / Peer to peer - Many of the clients available (andall of those mentioned here) are capable of file transfer. It would be a simple process for an individual to send a confidential document (such as an Excel file containing sensitive pricing or financial data)to a third party.

ii. Email - An internal user could email a confidential document to an unauthorized individual as an attachment.

iii. Web Mail - Gmail, Yahoo, and Hotmail are popular examples. It represents another way for an individual to leak confidential data, either as an attachment or in the message body.

iv. Web Logs / Wikis - are place where people can write their comments, thoughts, opinions and others on a particular subject. Inputs of the blogs are from thousands of individuals. Blogs might be used by somebody to release confidential information, simply through entering the information in their blog.

v. Malicious Web Page – Web sites that are either compromised or are deliberately.

vi. Hiding in SSL - A StatefullPacket Inspection firewall will not be able to examine the data as it will be encrypted. Consequently sensitive information may be leaked through this medium without detection.

vii. File Transfer Protocol (FTP) - FTP is probably more likely to be used in intentional leakage than unintentional leakage, due to the fact that uploading a file to

an FTP server is generally not something an average user performs on a daily basis, nor would do inadvertently, as compared to attaching a file to an email.

viii. Removable Media / Storage - Copying a document onto a USB and share with unauthorized user.

ix. Security Classification Errors - It is conceivable that an individual with Top Secret clearance may either intentionally or inadvertently send a Top Secret document to another individual with only “Classified” clearance.

x. Hard copy - Print out the data and walk out of the office with it in their briefcase. Or, they simply place it in an envelope and mail it.

xi. Cameras – Technology that have a camera built in, perhaps with up to 2 mega pixels or more. The photo could then be sent by email or Mobile Messaging directly from the telephone.

xii. Inadequate folder and file protection - If folders and files lack appropriate protection then it becomes easy for a user to copy data and distribute to unauthorized user.

xiii. Inadequate database security – Weaknesses in SQL programming can leave an organization exposed to SQL injection attacks, or allow inappropriate information to be retrieved in legitimate database queries.

2.2.2 MAF in Data Handling Isues

The official messages which is the confidential data in the MAF requires special requirements, proper handling as well as the strict compliances along with the laid down procedures as sanctify in MAF Staff Manual whereby the mishandling would result in congestion and delay of the intended information to be delivered safely (Defence Operations and Training Division, 2002). Confidential data handled

in accordance to its precedence consists of three main components (Defence Operations and Training Division, 2002):

i. Precedence Action which is inserted by the originator to indicate the relative order of information handling towards the recipients actions.

ii. Precedence Information which is inserted by the originator to indicate the relative order of information handling towards the recipient actions. In here, the precedence degree will always need to be the same or lower than the precedence action and will be assigned as "Routine" by default.

iii. Degree of Precedence which involve the precedence of "Flash", "Immediate", "Priority", and "Routine". Detail explanation of confidential information degree of precedence is attached in Appendix A.

The fundamentals of service writing and staff procedures that relate to staff work for adoption in the MAF are portrayed in MAF Staff Manual (Defence Operations and Training Division, 2002). MAF categorises the security classification according to the grade of particular security information contained in documents. It indicates the degree of jeopardising the national or international security that resulted from its illegitimate disclosure along with the conservation against such an exposure. Supplementary to these security classifications are:

i. Top Secret – Information and material, the unauthorised disclosure of which would cause exceptionally grave damage to the nation.

ii. Secret – Information and material, the unauthorised disclosure of which would damage the interests of the nation.

iii. Confidential – Information and material, the unauthorised disclosure of which would be prejudicial to the interests of the nation.

iv. Restricted – Information and material, the unauthorised disclosure of which would be undesirable to the interests of the nation.

These security classifications reflect the urgency in handling of the classified information whether it is restricted, confidential, secret or top secret in any cases. Information that does not involve national interests may still require a degree of protection or special handling. It also portrays the huge significant damage in mishandling the pertinent information to the nation.

In MAF, Secretariat, A. (2013) has classified the disclosure of the confidential information as any activities whether intentionally or not which lead to the dissemination of military information, criticising or giving opinions openly on any government policies, provoking on sensitive issues or sentiments that raised hatred of others against the government policies as well as other related matters which may affect the security of the country. The confidential information related can be categorised of any text documents of various format, any form of pictures or images in various format, any form audio visual, any form of military unit's mobility status and activities, any sketches of digital images and encyclopaedia provided by public as well as personal information such as pictures, immoral conduct or activities which will reflect a negative image on the MAF. The identified techniques of confidential information dissemination are listed as:

i. Upload, post, update or transmit any kind of classified or classified documents.

ii. Download any application forms or documents that are not known to its security.

iii. Discuss and participate in any form of forums on issues that may affect the safety and harmony of the country.

iv. Provoke or offer any form of provocation.

v. Using public email for an official business.

vi. Use of public facilities for the purpose of hosting the unit's official website.

vii. Allowing third parties outside the MAF organization to carry out activities of penetration testing, information and communication technology audit, and access to internal systems without permission from Defense Intelligence Staff Division (DISD).

2.3 Human Factor in Information Security

Information security is made up of technology, process and people elements(Lean-ping & Chien-fatt, 2014). Figure 2.2 illustrates the aspects of information security and how it related each other's. Technological is when the implementation or introduction of latest security software, hardware, firewall, encryptionmethodology, network protection scheme or regular penetration test to the system were addressed. The procedural or process aspects of information security can be introduced or enforced through compliance to policies, regulatory requirements, checklists, standards or security certification process. On the other hand, people aspect of information security is very subjective.

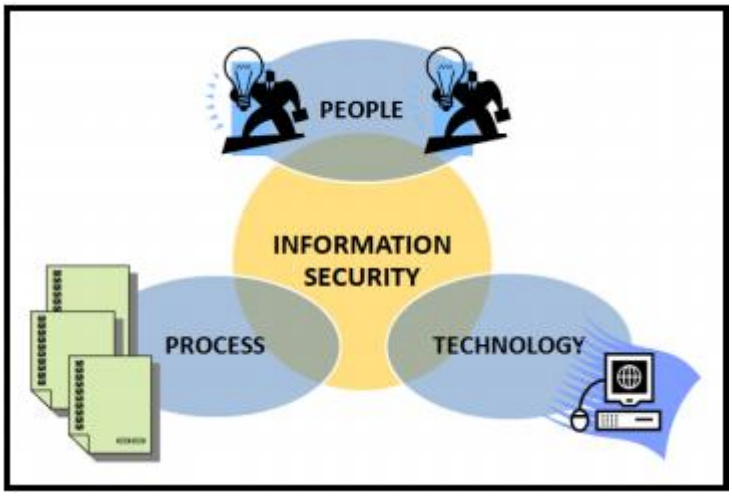


Figure 2.2: Aspects on Information Security (Lean-ping & Chien-fatt, 2014)

The current state of information security compliance in workplaces isdeteriorating. In many cases, human factors were attributed as the cause of the problem. Humans are well known as the weakest link in the security chain (Zakaria

& Katuk, 2013). Figure 2.3 illustrates the Security Framework proposed by Deloitte and it is also stressing on the relationship between governance, people, policy and technology.

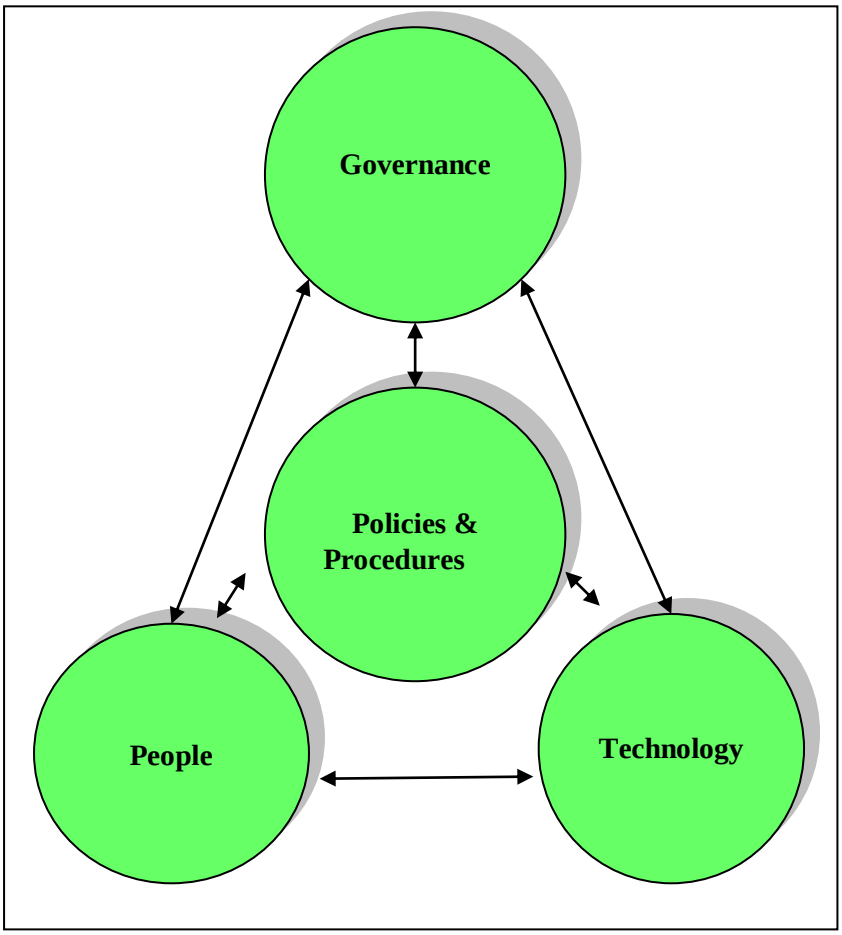


Figure 2.3 Security Framework (Marko Van Zwam, Martijn Knulman, 2012)

Many of the processes needed to protect these information assets are, to alarge extent, dependent on human cooperated behavior (Van Niekerk & Von Solms,2010). For successful data leakage prevention, it is it is crucial to make users the first line of defense. A user driven data leakage strategy will start with the user, alerting them to potential data loss that could be happen in their daily routine, and giving them knowledge to manage the tools to fix policy violations before they happen (Titus, 2008). Data governance as a first layer of defense in the DLP Conceptual Model proposed. Figure 2.4 clearly demonstrated the relationship between technology and the human role to ensure information security of an organization are prevented.

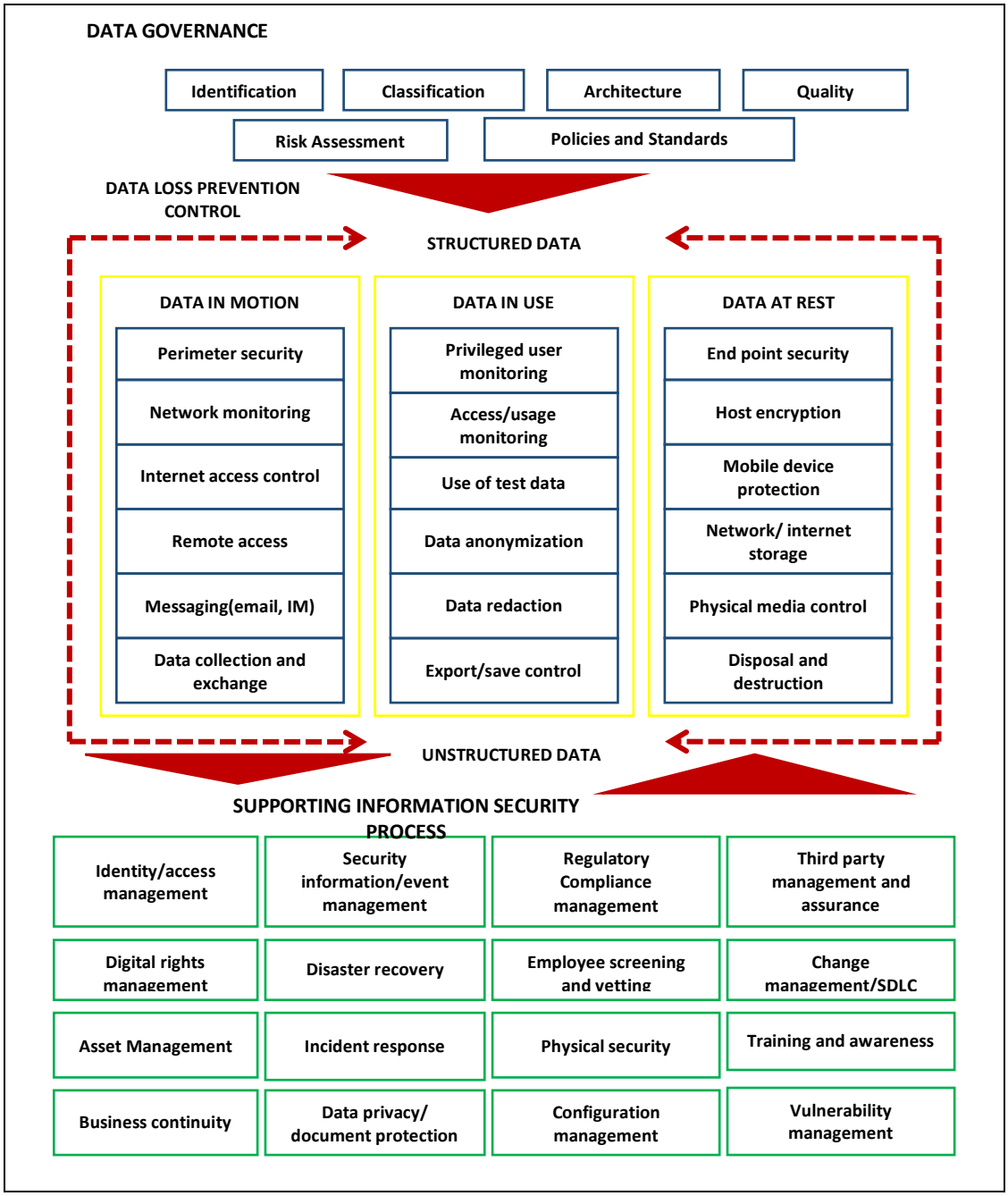


Figure 2.4 DLP Conceptual Model (Young, 2011)

From the above model, is clearly demonstrated the relationship betweentechnology and the human role to ensure information security of an organization. Information security starts with a strong governance structure (Marko Van Zwam, Martijn Knulman, 2012). This DLP controls cannot operate effectively in a vacuum. In order for a DLP program to be effective, the links to other

information security processes must be understood so that multiple layers of defense are established and monitored. For example, effective logical access controls may be in place, but if physical controls fail and sensitive hard copy information is removed from your facilities, data loss still occurs. Likewise, if changes to your infrastructure are not carefully controlled, existing DLP controls can become ineffective. Theareas listed in the "Supporting information security processes" section of the DLP conceptual model will help you identify key controls outside of the DLP program that can impact your overall effectiveness in managing data loss risks. Figure 2.5 shows the framework of IT governance effectiveness.

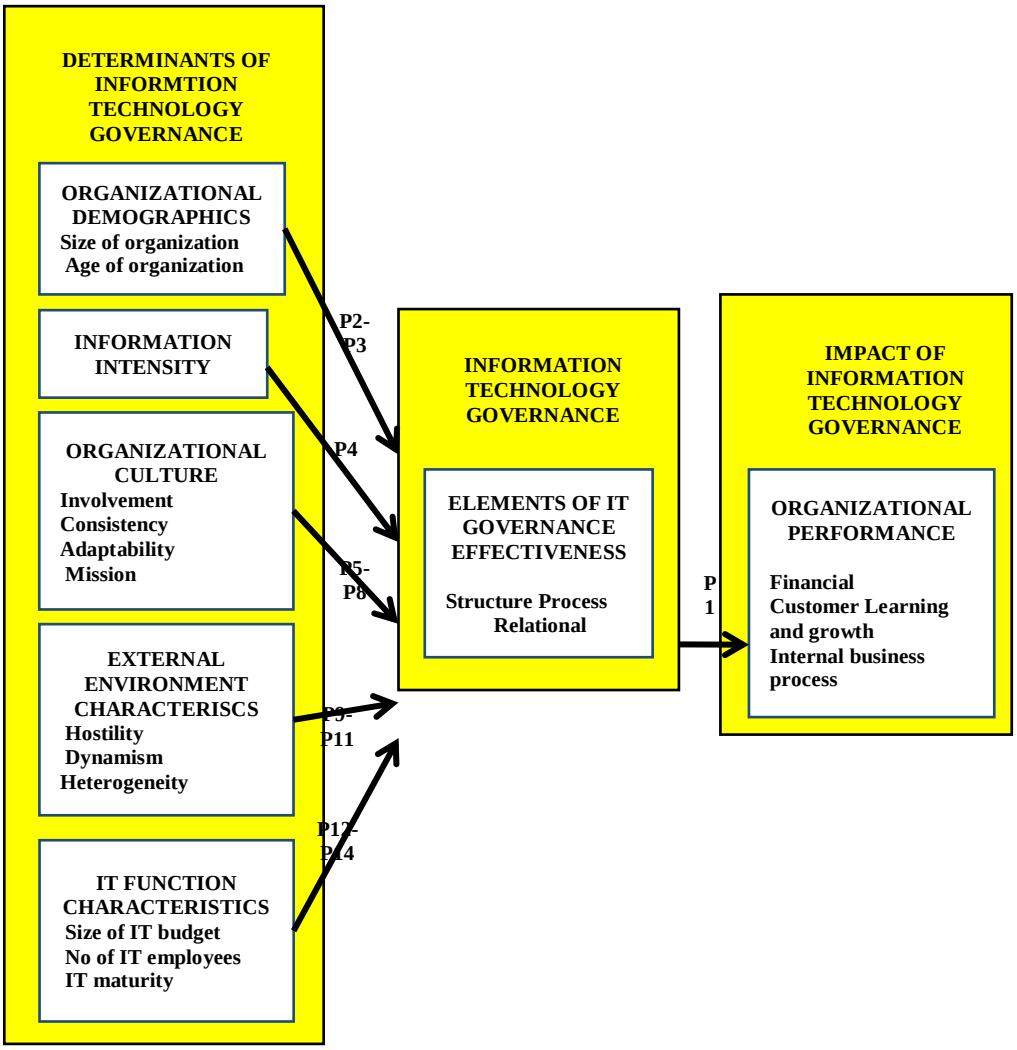


Figure 2.5 Framework of IT Governance Effectiveness (Mohamed & Singh, 2012)

IT governance is part of corporate governance cited as a means to helporganizations manage risk and protect themselves from technology-related losses. The importance of IT governance is evident through the attention it receives from scholars and practitioners. As noted previously, the focus of extant IT governance effectiveness research is separated from its link to determinants and impacts (Mohamed & Singh, 2012). It is essential that DLP controls and supporting information security controls are implemented and that the effectiveness of these controls is monitored over time. Having a structured data loss risk management program and a clear set of controls to mitigate data loss risks can provide a holistic view of data loss potential across your organization. The DLP conceptual model can also aid in building a customized data loss risk dashboard and performing current-state assessments.

2.4 Common Behaviors Resulting in Potential Risk of Data Leakage

Although governments are actively focused on fighting and preventing cybercriminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges to the implementation of cyber regulations in any country (Herhalt, 2011). The implications for practitioners are potentially significant. In order for an organisation to implement effective information security, it is essential to gain an understanding of all the employees within the organisation. In addition, compliance with security policies is necessary and, in some cases, this compliance needs to be demonstrated by either the information security function or the risk management function within an organisation in order to justify their activities (Stephanou, 2008).

Ricky M. Magalhaes in his article list human behavior that resulting to the data leakage are as below (Magalhaes, 2011) :

i. Speaking loudly in public areas about sensitive corporate data

ii. Failing to log off laptops

iii. Leaving passwords unprotected

iv. Accessing unauthorised websites

v. Loss or theft of corporate devices (Laptops, Mobile phones, Portable hard drives)

vi. Loss or theft of personal devices now also being used for corporatepractices

vii. Thumb drives

viii. Optical media

ix. Email

x. Instant messaging

xi. Access control both physical and logical

xii. Lack of encryption

xiii. Lack of two factor authentication

xiv. Lack of remote access control

In many cases, data breaches happen because the user was not aware of theimpact of their actions. Users may be unfamiliar with corporate policy, or they may not understand the larger compliance picture in regulated environments such as financial organizations. Sometimes it's simply a matter of underestimating the consequences of going against policy – such as sending confidential documents to ahome email address to complete the project after regular business hours(Titus,

2008). Table 2.1 illustrate common unintentional data loss or data leakage regarding people, process and technology.

Table 2.1 : Common Unintentional Data Loss Theme (Young, 2011)

People	Process	Technology
Employees do not clearly understand or feel accountable for the protection of sensitive data.	Data protection, data classification and acceptable use policies do not clearly articulate: ‣ The controls that should be implemented for securely sending sensitive data to third parties ‣ Whether employees may send sensitive data to home computers and personal email accounts ‣ The specific data that is considered sensitive and requires data protection controls	Current remote access tools are not flexible enough to support the business, resulting in users employing alternative approaches, such as emailing documents to their personal email accounts, to enable working from home and remote locations.
Training and awareness programs do not focus enough on protecting sensitive data, appropriate use of email and the internet, use of security tools such as file encryption and each employee's personal responsibility for complying with information security/data protection policies.	Process owners have not assessed their methods in which sensitive data is shared with third parties to evaluate information security risks.	Content-aware email encryption tools are not effectively used to automatically require encryption of emails containing sensitive data, such as account numbers.
Employees feel that there is no risk involved in breaking the rules (i.e., "no one is watching so I will not be caught").	Without an ongoing DLP monitoring program, policy violations cannot be identified efficiently, and the success of policy communications, training and awareness programs and technical controls is not measurable.	Secure links between the company and its third parties are not in place to enable encrypted email or other secure transmission methods.

2.5 Security Awareness

User negligence is considered as one of the critical factors in the informationsecurity context. Creating awareness among users is proving to be one of the efficient ways of fighting negligence (Yayla, 2011). Organizations should expect to see a drop in policy violations as users become more security conscious. Users will become more familiar with corporate policy, and will also become more aware that their actions might be monitored. This will drive change in user behavior, contributing to an overall reduction in security incidents (Titus, 2008).

The main objectives of security awareness programs are making employeesaware of procedures, rules and regulation stated in the security policy and

making employees aware of security concerns (Yayla, 2011). Increasing users' awareness about security threats and computer-based controls such as authentications and antivirus systems will help them understand the severity of the threats and also increase utilization of these control mechanisms. However, given their importance, awareness programs constitute approximately 1% of security budgets in organizations (Richardson, 2009).

The security awareness program message has to be repeated quite often.Also, the procedures to report security incidents have to be clearly identified by the administration of the organizations. Bringing security awareness topics are crucial, however, equally important is to make employees be ready to identify and act responsibly when security incidents happen (Martinez, Turabo, & Cleal, 2010).

2.5.1 A Framework of Security Awareness and Information Security

Based on previous research, there are several frameworks being analyzed inorder to develop Security Awareness Model for Data leakage Prevention.Other models that can be used as a reference from the previous report are amodel of management effectiveness in information security. Figure 2.6 shows the model proposed that the relationship between top management support and perceived security effectiveness is partially mediated by user training, security culture, policy relevance and policy enforcement. Additionally, user training is positively associated with security culture (Knapp, 2005).

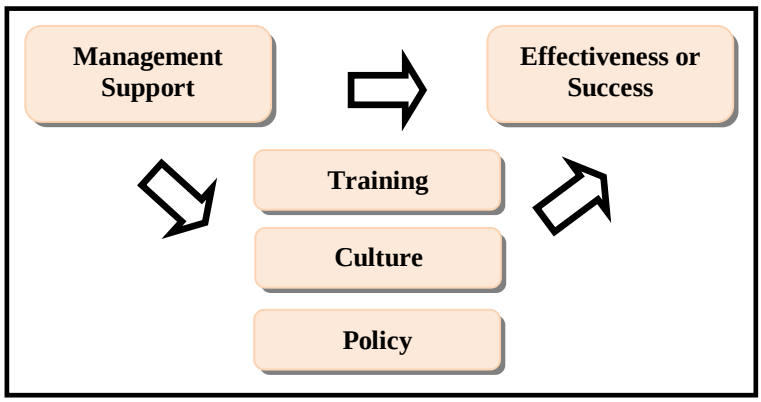


Figure 2.6 Model Of Managerial Effectiveness in Information Security (Knapp, 2005)

Another framework discussed evaluating ICT security awareness is Meansendsobjectives network for ICT security awareness framework (Kruger HA, L Drevin & Science, 2007). The framework starts with the identification of areas to focus on – these areas are then used to gauge employees' knowledge, attitude and behavior levels(Kruger HA, L Drevin & Science, 2007). Combined with certain system generated data, and appropriate importance factors, the employee surveys are used as input into the model to calculate awareness levels. In order for security awareness programs to add value to the organization and at the same time make a contribution to the field of security information, it is necessary to follow a structured approach to study and measure its effect.

A discussion on the identification of focus areas was also given. To do this,a value focused approach was followed and resulted in a network of relationships that suggests how means objectives may interact and influence fundamental objectives and ultimately the overall objective of maximizing ICT awareness. Brief notes on the use of the system generated data that may assist with the determination of security behavior was also presented.

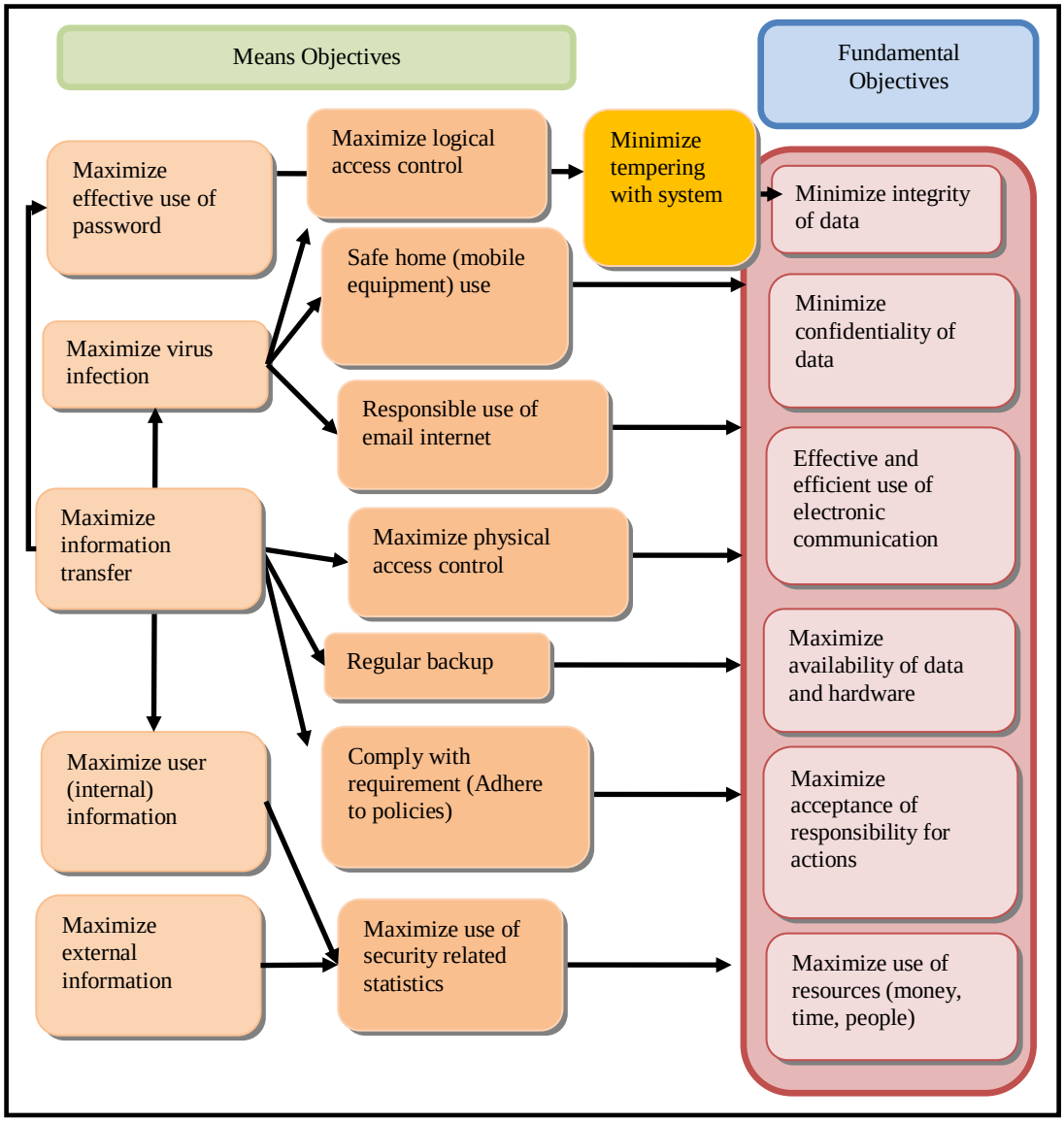


Figure 2.7 Means-ends objectives network for ICT security awareness (Kruger HA, L Drevin & Science, 2007)

The following discussion focuses on a framework meant to control andmonitor insider threats to information security. As per the literature, insider threats are divided as intentional and unintentional. In order to reduce intentional insider threats, the suggested framework draws connections to the organizational behavior, criminology and psychology literatures. Increasing employee integration and commitment, using deterrent measures, and finally implementing technology-basedcontrols are suggested as potential measures in order to control and monitor intentional threats.

In addition, unintentional threats can be monitored or mitigated byincreasing employees' intrinsic motivation, providing proper trainings for security tools, implementing them with the high level of usability, adjusting time pressure and workload on employees, and lastly by increasing awareness among users and management (Yayla, 2011).

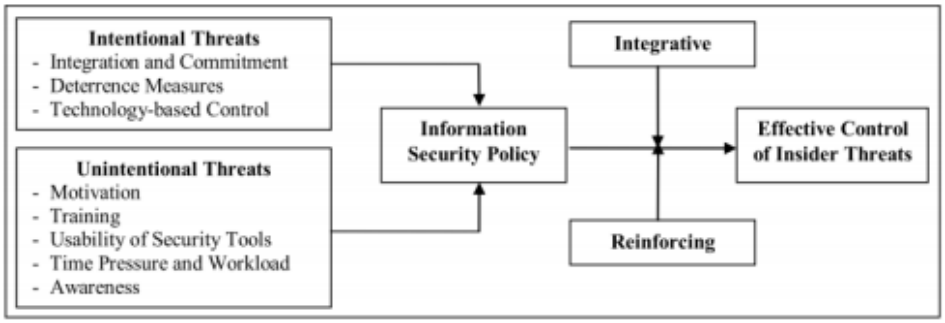


Figure 2.8 Framework for monitoring internal threats to security data (Yayla, 2011)

The following discussion focuses on analyzing methods for building a successful security awareness program and presented a set of propositions for the betterment the program. Figure 2.9 illustrate a Framework for implementing Security Awareness Program Issues.

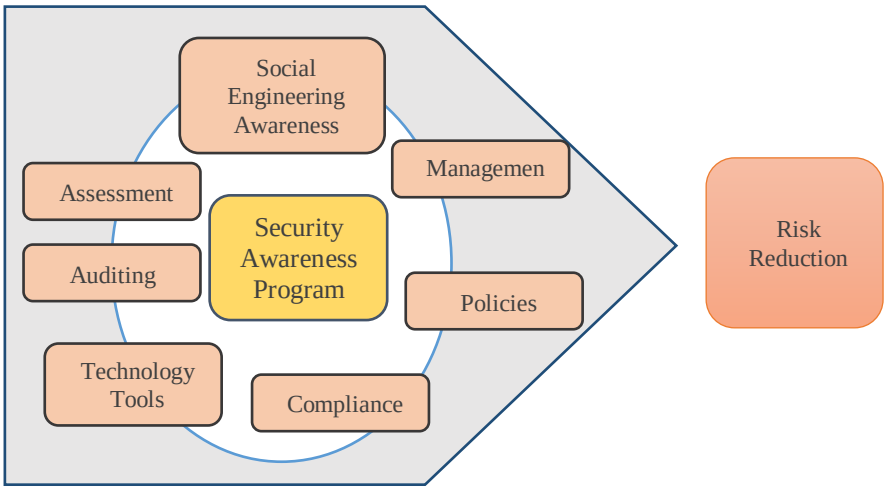


Figure 2.9 Framework for Implementation Issues Safety Awareness Program(Martinez et al., 2010)

The following discussion is focusing on the important of Information Security Management (ISM) factors and cultural factors in Saudi Arabia that have not been widely addressed in the discipline specific or related literature. This research believes that there is a gap in terms of addressing the influences of bothISM factors and cultural factors on the adoption of security culture in any organization. ISM factors were incorporate into three themes such as corporatecitizenship that include information security awareness and training programs, legal and regulatory environment that include ISM standardization and best practices and information security policy, and corporate governance that include top management support for ISM, information security compliance and information security risk analysis. In addition, a cultural theme that include national and organizational culture that has a strong influence on the adoption of security culture. Therefore, we aim to address the gap in knowledge about ISM factors and cultural factors that will lead to the implementation and the adoption process of IS cultural and practices in Saudi Arabia. We plan to test the conceptual framework explicated in figure 1 which results from our literature analysis in a large-scale project consisting of a quantitative survey and in-depth interviews to examine the influence of the factors identified and their impact on adopting IS culture and practices in Saudi Arabia (Alnatheer & Nelson, 2009).

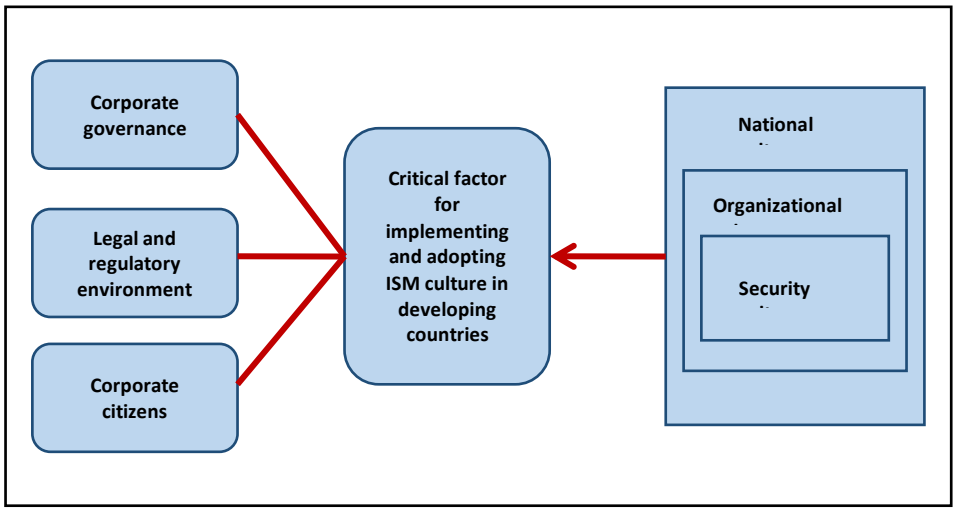


Figure 2.10 Factors for implementing and adopting IS culture and practices in Saudi Arabia (Alnatheer & Nelson, 2009)

The following framework is Conceptual Information Security Framework for Higher Education Institutions (HEIs**) .** The researcher highlighted five security elements are used to enforce the Information Security Framework (Ismail, Masrom, Sidek, & Hamzah, 2010). The security construct consist of five elements which is information security policy, risk management, access control, awareness and training and compliance. These elements influence to measure the effectiveness ofimplementing information security for higher education institution.

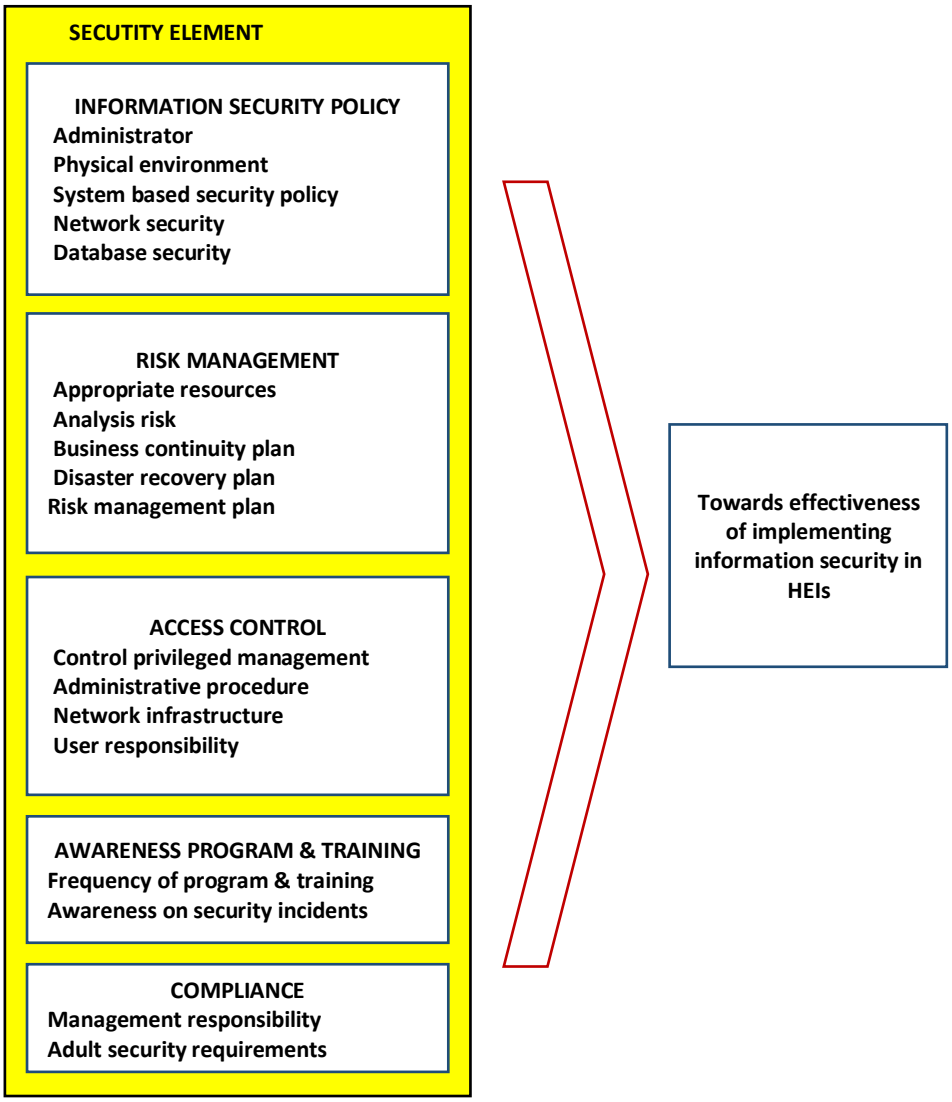


Figure 2.11 Conceptual Information Security Framework for Higher Education Institutions (HEIs) (Ismail et al., 2010)

Last frameworks discuss security culture delivers the way on how people react towards the information security in the organization. This researcher consolidated the key factors influencing information security cultures are categorized as behavioral, change management, information security awareness, organizational system, security requirements and knowledge. Result of testing shows that all elements that influence to the information security culture have a positive relationship with information security culture. Figure 2.12 illustrate Modelfor Factor Influencing Information Security Factor.

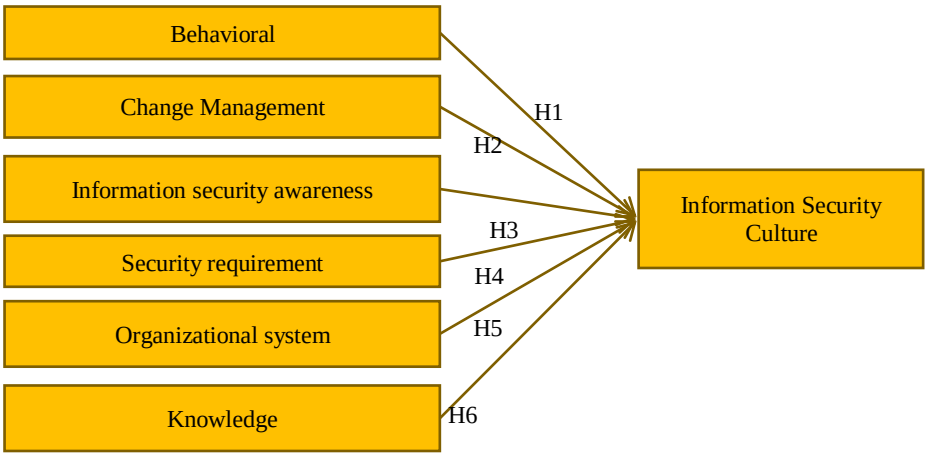


Figure 2.12 Model for Factor Influencing Information Security Factor (Hassan &Ismail, 2012)

2.6 Data Leakage in The Use of Social Media Attributes from Structured Literature Review (SLR)

Thorough findings, observation towards other research model, framework and attributes of data leakage from other fields retrieved from the SLR has then served as the basis as the references in initiation of the proposed model of data leakage prevention in the use of social media. The related attributes of data leakage prevention are identified which then being mapped into the model, framework as well as approach used in developing a proposed model which will be pictured in the next section. The SLR is used as the systematically, explicitly and reproducibly

method in conducting the literature review (Okoli and Schabram, 2010) to methodically identify, evaluate or assess and synthesize or interpret all extant researches (Kitchenham and Charters, 2007; Okoli and Schabram, 2010) in order to provide answers to specific research questions while Petticrew and Roberts (2008) on the other hand stated that the SLR as a tool to provide the evidence in specific area with scientific summary. Following are the results of the SLR which consists of 4 attributes of from 7 studies which have met the criteria to be selected.

2.6.1 SLR Review Method

The review process of this research is following the SLR guidelines introduced by Kitchenham and Charters (2007), and Okoli and Schabram (2010). The available technology ethics applied in other fields to be adapted in the MAF are identified to fulfil the intention of this research. The phases and stages involves in conducting the review of the SLR are analogous as below:

i. Planning the review which consists the stages of review purpose identification, research questions formulation and review protocol development that describes the review strategies to be carried out for both planning and execution of the review.

ii. Executing the review which consists of relevant literature identification with comprehensive search, selection of primary studies based on inclusion and exclusion criteria followed by evidence synthesising.

iii. Writing the review which consists of formatting the report.

Changes in the review involved the protocol to be revised since the review itself is an iterative process. The phases involved are summarised in Figure 2.13.

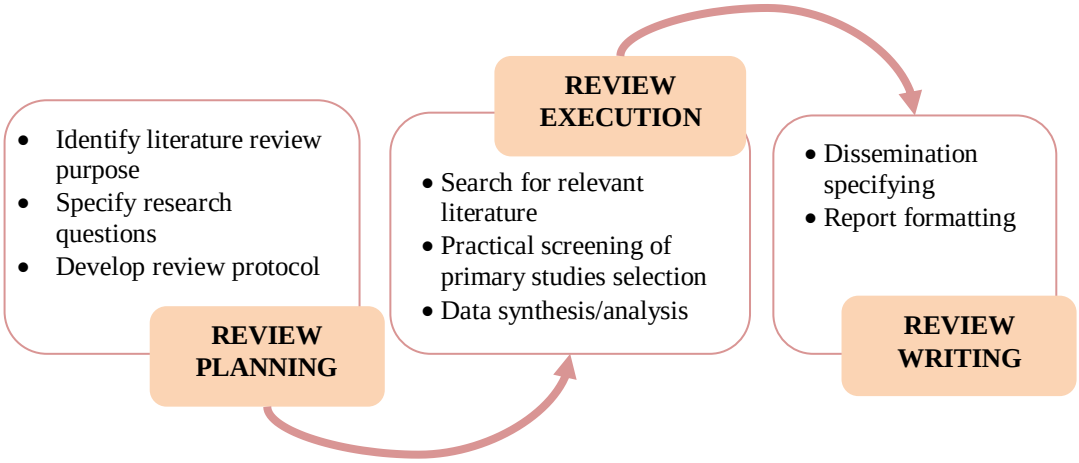


Figure 2.13 Phases and Stages of Systematic Literature Review

The research question will be specified in the following steps which involve in the review of this SLR. It lies in the review planning phase with further explanation of the SLR execution.

a. SLR Research Question

Research question plays the heart in governing the commission of the review as stated by Dyba *et al.* (2005). In this review, Petticrew and Roberts (2008) criteria for formulation of research question is followed which comprised of five elements that are known as population, intervention, comparison, outcomes and context (PICOC). Details of each element used in this review are as below:

i. Population delineates the investigation target group.

ii. Intervention construes the researcher issues or aspects of interest.

iii. Comparison illustrates the investigation aspects where Intervention is compared.

iv. Outcome determines the Intervention effects.

v. Context specifies the investigation environment and settings.

The PICOC structure for the research question formulation used in this research is described in Table 2.2.

Table 2.2: PICOC Structure of Research Question

Criteria	Scope
Population	Personnel
Intervention	Data leakage factors
Comparison	Other fields
Outcomes	Data leakage factors attributes
Context	Reviews of any studies on data leakage in the use of social media

This SLR primary focus is to understand and identify the data leakage factors within the other fields which would be the primary research question of this SLR. It is later presented in chapter 2 under the Attributes that Effect Data Leakage section in which the results are extracted from the evidence synthesis later in this chapter. It would be beneficial in answering the first research question of this whole research apart from this review research question itself. The initial skeleton of the outcomes of this SLR is depicted in Figure 2.14 which will be developed as the conceptual model for data leakage after the synthesizing stage.

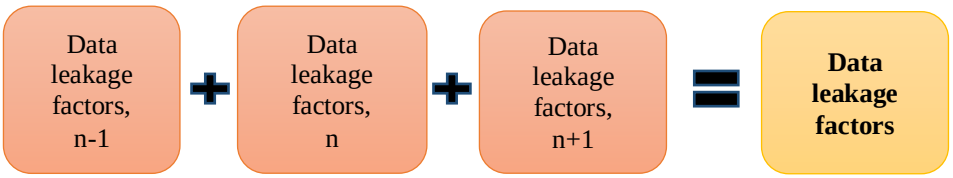


Figure 2.14 Skeleton of Conceptual Model for Data Leakage Factors

b. Identification of Relevant Literature

The discovery of the literatures to be considered in conducting the SLR require suitable research strings in ensuring the wide coverage of potential existing studies which is mainly the journal and conference papers. Strategy in composing the comprehensive and exhaustive search strings has followed Kitchenham and Charters (2007) derivation guideline whereby:

i. PICOC major terms derivation as conducted in previous stage

ii. Synonyms and alternative words are constructed (Table 2.3)

iii. Incorporate Boolean "OR" in constructing synonym and Boolean "AND" in linking the major terms (Table 2.4)

Table 2.3: Synonyms and Alternatives

Terms	Alternative Term
Data Leakage	Information Leakage
Social Media	Social Networking

Table 2.4: Concatenation of Alternative Words with Boolean OR

No.	Concatenation Results
1.	("Data Leakage" OR "Information Leakage")
2.	("Social Media" OR "Social Networking")
3.	("Armed Forces" OR "Military forces")
Possible words concatenation with Boolean AND	
("Data Leakage" OR "Information Leakage") AND ("Social Media" OR "Social Networking") AND ("Armed Forces" OR "Military forces")	

b (i) Data Sources

The primary search involved three online databases as the data sources which are IEEEXplore Digital Library, ScienceDirect, and Taylor & Francis Online. The selection of databases was based on University Teknologi Malaysia's subscribed online databases. This step of referring to different databases is recommended by Khan *et al.* (2011) in preventing bias in the review.

b (ii) Search Strategy

The initial primary searches string are Data Leakage, Social Media and Armed forces which is then being further constructed using the Boolean "OR" and Boolean "AND" to permit synonym and word class variant results with the search string of ("Data Leakage" OR "Information Leakage") AND ("Social Media" OR "Social Networking") AND ("Armed Forces" OR "Military forces") which the results findings are summarised in Table 2.5.

Table 2.5: Initial Databases Primary Searches String Results

Database/ Search String	IEEE Xplore	Science Direct	Taylor& Francis	Total Searches
("Data Leakage" OR "Information Leakage") AND ("Social Media" OR "Social Networking") AND ("Armed Forces" OR "Military forces")	3	1004	1962	2969
Second String Searches: ("Data Leakage" OR "Information Leakage") AND ("Social Media" OR "Social Networking")	27,000	6806	6854	40,660
Third String Searches: ("Data Leakage" OR "Information Leakage")	191,000	234,109	57,817	482,926

The observation from the initial search string conducted using the full search string was three out of three databases were the Taylor & Francis Online Database

has returned 1962 results studies, 1004 for Science Direct and 3 for IEEEXplore Digital Library related articles.

In addition, the specificity, as one of the major issues in conducting the SLR highlighted by Petticrew and Roberts (2008) would appear as there were lesser articles retrieved as the string are long that can be seen from the first and the second string development. So for that reason, the third string searches of ("Data Leakage" OR "Information Leakage") was determined to be used as the initial articles selection and to be considered using inclusion criteria that is seemed to give more results in terms of articles finding in each databases used that is tailored to the primary RQ in this review. The results for the third string searches are 57,817, 234,109, and 191,000 of studies for Taylor & Francis Online, ScienceDirect and IEEEXplore Digital Library respectively. The fields selection are filtered according to Computer Science for ScienceDirect, Computer Science, Behavioral Sciences, Information Science and Social Sciences for Taylor & Francis Online, and all results from IEEEXplore Digital Library which are all being filtered according to the articles availability which have been subscribed by Universiti Teknologi Malaysia. Table 2.6 shows the final articles selection based on initial articles selection that have conformance to the predetermine inclusion criteria.

Table 2.6: Final Articles Selection

Database	Number of Articles found based on Primary Searches	Number of Selected Articles
IEEEXplore Digital Library	3	3
ScienceDirect	1004	4
Taylor & Francis Online	1962	0
Total	**2969**	**7**

2.6.2 Selection of Related Studies

This review adopted the inclusion criteria which involved articles of journals and conference papers that are published within the year of 2009 to present, which is six years back articles. The articles selected are based on articles that are written in English. The articles targeted were those on data leakage, social media, armed forces and other fields that serve as full text articles which were used as the initial primary string searches while articles that did not fulfil the inclusion criteria will be deemed as the exclusion criteria and will not be inserted in the data synthesising. The exploration of articles' title and abstract are done thoroughly such that the eligibility criteria of inclusion and exclusion criteria are measured. The full text is referred if the articles' abstract do not provide sufficient relevant information of the particular articles. Further discussion on these studies selection was described in identifying relevant literature which is under section 2.6.3 of Review Outcome.

2.6.3 Review Outcome

Analysis of the literature search results is presented in Table 2.7 where the breakdown of literature searches from four online databases is stipulated. The duplicate articles found were eliminated along the process of inclusion criteria selection.

Table 2.7: Article Searches Breakdown

Database	Total Articles found for Screening, A	Total Irrelevant Articles based on Inclusion Criteria (Screening 1), B	Total Irrelevant Articles based on Inclusion Criteria (Screening 2), C	Total to be Reviewed after Inclusion Criteria, D
IEEEXplore Digital Library	3	0	0	3
ScienceDirect	1004	998	2	4
Taylor & Francis Online	1962	1900	62	0
Total	**2969**	**2898**	**64**	**7**

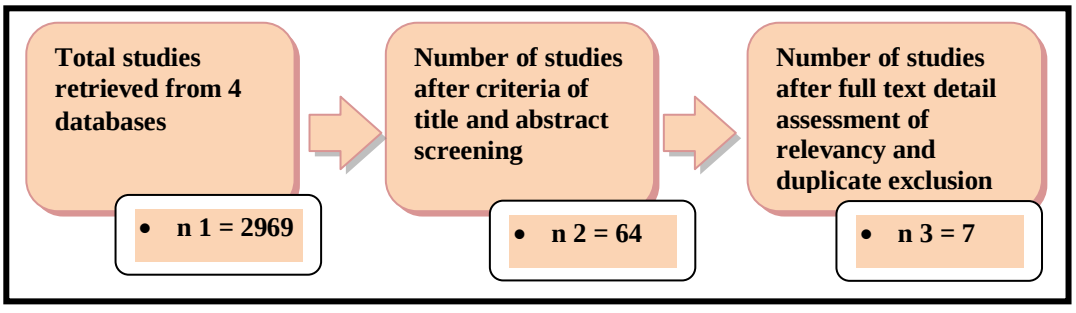


Figure 2.15 Identifying Relevant Literature

2.6.4 Synthesising of the Evidence

The identified attributes of data leakage which is the primary research questions are presented in Chapter 2 in section Attributes that influencing data leakage in the use of social media from SLR and would be served as the attributes to be inserted in the skeleton of the proposed conceptual model of factors influencing data leakage in the use of social media. The outcomes details which have been derived from the review outcome are presented in Table 2.8.

Table 2.8: Evidence Synthesising Findings

No	Framework	Author	Construct
1.	Model Of Managerial Effectiveness in Information Security	Knapp, 2005	Computer Usage Behavior , Security Awareness , Policy Acceptance and Understanding
2.	Means-ends objectives network for ICT security awareness	Kruger HA, L Drevin & Science, 2007	Computer Usage Behavior , Security Awareness
3.	Framework for controlling insider threats to information security	Yayla, 2011	Computer Usage Behavior , Security Awareness, Security Education and knowledge
4.	Framework for Implementing Security Awareness Programs Issues	Martinez et al., 2010	Security Awareness, Security Education and knowledge
5.	Factors for implementing and adopting IS culture andpractices in Saudi Arabia	Alnatheer & Nelson, 2009	Computer Usage Behavior , Security Awareness , Policy Acceptance and Understanding
6.	Conceptual Information Security Framework for Higher Education Institutions (HEIs)	Ismail et al., 2010	Security Awareness, Security Education and knowledge, Policy Acceptance and Understanding
7.	Model for Factor Influencing Information Security Factor	Hassan & Ismail, 2012	Computer Usage Behavior , Security Awareness, Security Education and knowledge, Policy Acceptance and Understanding

2.7 Summary of Related Variable

From the review, four (4) factors emerged as construct that influence data leakage in the use of social media among Malaysian Armed Forces personnel.Table 2.9 shown the related research on data leakage.

Table 2.9: Related Research On Data Leakage Prevention

No	Framework	Author	Construct			
			Computer usage behavior	Security education and knowledge	Policy acceptance and understanding	Security awareness
1.	Model Of Managerial Effectiveness in Information Security	Knapp, 2005	/		/	/
2.	Means-ends objectives network for ICT security awareness	Kruger HA, L Drevin & Science, 2007	/			/
3.	Framework for controlling insider threats to information security	Yayla, 2011	/	/		/
4.	Framework for Implementing Security Awareness Programs Issues	Martinez et al., 2010		/		/
5.	Factors for implementing and adopting IS culture and practices in Saudi Arabia	Alnatheer & Nelson, 2009	/		/	/
6.	Conceptual Information Security Framework for Higher Education Institutions (HEIs)	Ismail et al., 2010		/	/	/
7.	Model for Factor Influencing Information Security Factor	Hassan & Ismail, 2012	/	/	/	/

2.8 Proposed Conceptual Model for Data leakage Model in The Use of Social Media in MAF

Based on the previous research, there a several research can be guidance inconstructing the Model for Data leakage Model in The Use of Social Media in MAF. Most of the researchers agree that awareness plays an important role in ensuring the security of information in an organization. Employees need to be trained and educated on security awareness to let them aware and update with the information security world. Information security is made up of technology, process and people elements. Changing in human knowledge and awareness is influential to the prevention data leakage in the organization. Technology alone is useless without the involvement of human knowledge.

Based on the literature review, there is no specific model or theory use for developing Model for Factors of Data leakage Prevention in The Use of Social Media in MAF. However, four factors that influence to data leakage prevention have been identified. Hence, this study suggested four important components that influencing Factors of Data leakage Prevention in The Use of Social Media in MAF. Figure 2.16 shows the proposed framework based on the findings from the literature review.

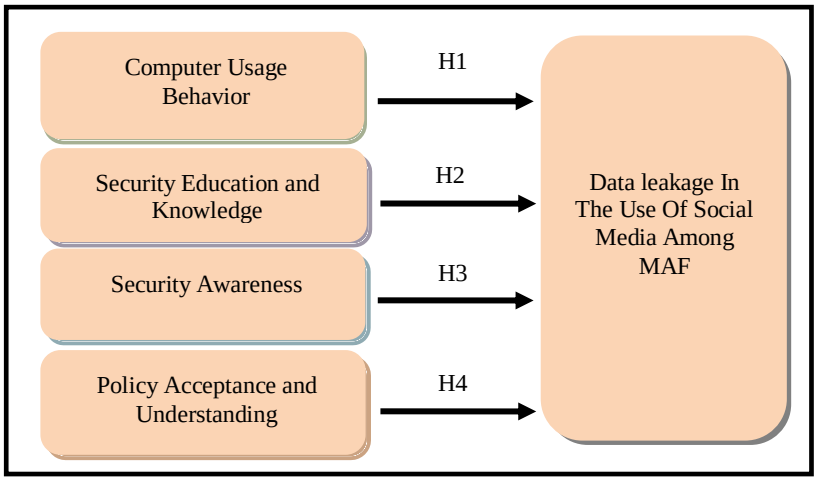


Figure 2.16 Proposed Conceptual Model Data Leakage Model In The Use of Social Media For MAF

Therefore, the following hypothesis is proposed based on literature:

i. Hypothesis 1: There is a positive significant relationship between Computer Usage Behavior and Data leakageIn The Use Of Social Media Among MAF.

ii. Hypothesis 2: There is a positive significant relationship between Security Education and Knowledge Data leakageIn The Use Of Social Media Among MAF.

iii. Hypothesis 3: There is a positive significant relationship between Security Awareness and Data leakageIn The Use Of Social Media Among MAF.

iv. Hypothesis 4: There is a positive significant relationship between Policy Acceptance and Understanding and Data leakageIn The Use Of Social Media Among MAF.

2.9 Summary

This chapter illustrates the literature review that has been made prior to the research in order to help the researcher in answering the research objectives of this whole research. By referring to previous work, this research will focus on awareness and human factor issue to prevent data leakage in MAF. These factors must be fortified in an arrangement in order to secure all the organizations are educated with the security issue. Technology and process alone are useless without human involving coordinating them. Four components have been identified in order to see the relationship with the factors of data leakage prevention. The proposed conceptual model is also presented in this chapter. In the next chapter, which is chapter 3, all the phases and stages in conducting the research will be explained which will be the full skeleton of the development of this research.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the activities that have been conducted throughout the research which consists of nine sections. The discussion will highlight in step and process done undertaken to design and develop a model for factor influencing data leakage in the use of social media among Malaysian Armed Forces personnel. Section 3.1 is the introduction of this chapter. Section 3.2 described the research operational framework. Detail discussion of each phases are resumed in section 3.3 that covers the Information Gathering and Project Planning phase, Section 3.4 on Design phase, Section 3.5 on the Implementation phase, Section 3.6 on the Analysis phase, and followed by Section 3.7 of Report Writing phase. Section 3.8 continues with a research deliverable, and the chapter ends with section 3.9 which summarised the chapter.

3.2 Research Procedure

The research procedure indicates the steps involved in the research process that have been identified from the beginning of the research started from the information gathering and project planning up to the report writings. Figure 3.1 depicted the research procedure for this research development.

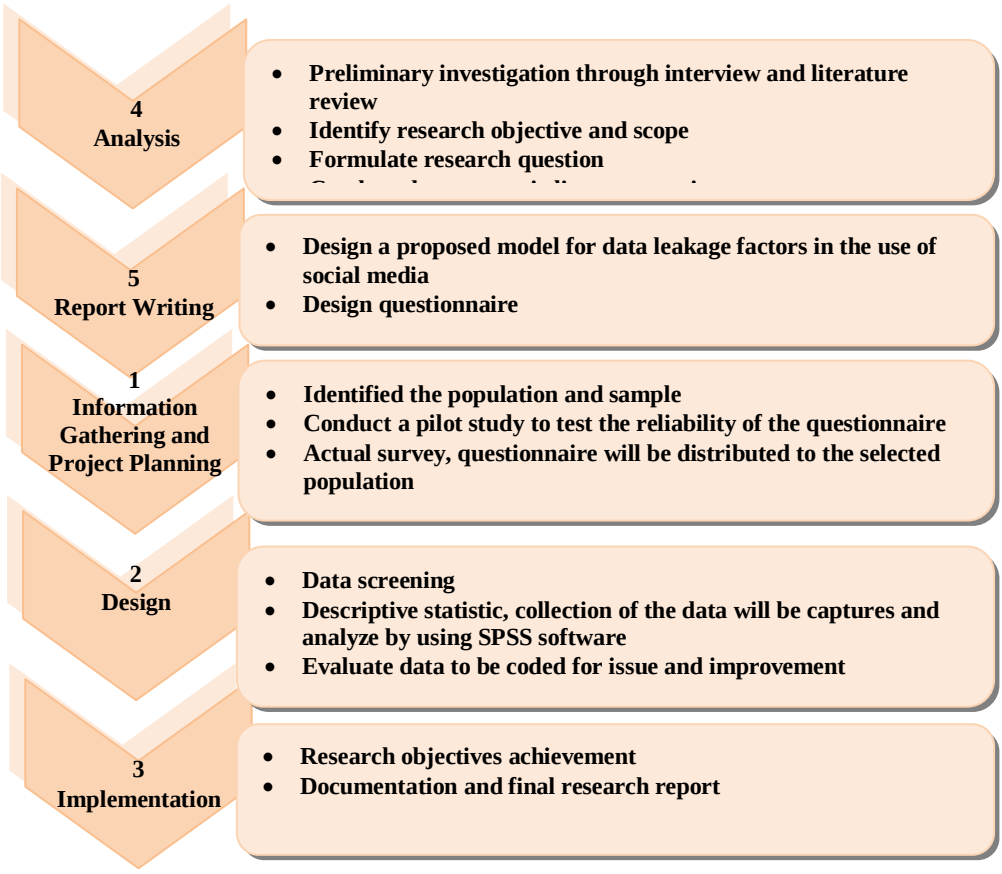


Figure 3.1 Research Procedure

There are five phases involved in the research process. Each phase will be examined in section 3.3 for information gathering and project planning phase, section 3.4 for design phase, section 3.5 for implementation phase, and section 3.6 for analysis phase followed by section 3.7 for report writing phase accordingly.

3.3 Phase 1: Information Gathering and Project Planning

Among all, the information gathering and project planning phase is first to be conducted in which to support the idea of the research topics before further construction. There are two stages involved which are performing the preliminary investigation by conducting the Literature Review from the related fields, and preliminary interview from the selected personnel to gather the experiences in the topic covered as well as by performing the Systematic Literature Riveiw (SLR). The

details are discussed in the following subsections. Intentionally, it would help the researcher in finding the gap exists in the current researches field which helps the derivation of the factors influencing data leakage attributes to be served as the input for the model designation on the next stage.

3.3.1 Preliminary Investigation

The preliminary investigation involves: First, conduct the Literature Review to find out the statement of the problems, initiate the research objectives gathered from the problems identified as well as assignments of the scope, second, conduct the independent interview sessions among two selected personnel from the Armed Forces in order to evaluate the significance of the research to be performed. It has been conducted by using non-structured questions as in Interview Outline (Appendix A) to gather the information and have further knowledge on the factors of influencing data leakage in the use of social media that involved in the MAF particularly. It is with the intention to assist the MAF organization in identifying the data leakage attributes involved among the Armed Forces personnel in the use of social media. This process is important to provide as supportive details and strengthen the purpose of the research development. Two of the selected interviewees agreed to participate in the interview. The selected interviewees and their background are described in Table 3.1 as follows.

Table 3.1: Interviewees' Profiles for Preliminary Investigation

Interviewee	Current Position	Positions/ Years of Handling	Years of Service
A	Staff Officer 1(SO 1) System in Joint Force Headquarters responsible for all Information Technology Systems in strategic and electronic communications for joint forces and overseas mission	• Commanding Officer (CO) Trunk Communication responsible for the operation of Defence Electronic Messaging System (3 years) • SO 1 Operation and Training RSR headquarters responsible for IT system, communication and electronic for the Army (3 years) • CO of 3rd RSR responsible for south system operational and communication (3 years)	33
B	Serves concurrently as Chief Supervisor of Cyber Monitoring Team, Army Web Master and Army System Administrator	• Army Web Master (14 years) responsible in developing and administering Army portal • Army System Administrator (14 years) responsible in continuous development and administering all Army Systems • Chief Supervisor Blog Monitoring Team (14 years) responsible in collecting and analysing information about army from outside the organisation *14 years is a concurrent responsibilities assigned	23

Based on the findings from these preliminary investigations which is the interview sessions on data leakage in the use of social media involved in the Armed Forces has demonstrated that both interviewees A and B strongly agreed upon the selected topic to be conducted due to the negative impacts of current trends regarding wide dissemination of confidential information outside the Armed Forces organisation especially throughout the technology of internet and mobile application. It is believe to be resulted from the lack of attitude that affect the secrecy of confidential information handling in daily works.

Furthermore, the newly established branch of Army Cyber Monitoring Team that was launched in December 14, 2014 recently as well as the Navy and Air Force of Navy Cyber Monitoring Team and Air Force Cyber Monitoring Team respectively

demonstrated the higher superior of the MAF towards preventing and monitoring initiative to curb data leakage accredited from version 1 of AFGI as issued by Secretariat, A. (2013) that has been authorised by the Chief of the Armed Forces which was released in January 14, 2013. The instruction designation is to oppose the confidential information of the Armed Forces from leakage via cyber platform which has reflected the current technology being used. Further specific instruction is then being issued as the Armed Forces initiative which highlights the media social usage guidelines for the Armed Forces that has consequently released on May 28, 2013 that has been signed by the Chief Staff of the Armed Forces which further expand the attribute of media social usage guidelines that also refer to the AFGI.

Reports of Cyber Monitoring in 2015 have shown that the shared information through media social happened to be the current trends in the Armed Forces organisation. Example of one of the case reported from the Army Cyber Monitoring Team is attached in Appendix C. All reports from the services teams will be submitted to Cyber Defence Department, Intelligence Branch and the respective monitored personnel department to implement further recommended actions by first, advising the personnel and publishing the prohibition to upload the confidential contents to the social media in part one orders which is the instruction medium for each unit. Failure to comply with such directives will result the personnel to be charged in accordance section stated in Armed Forces Act's (1972).

These have shown that the information exploitation has lead strategic management has look vigorously and has acquainted the responsible departments mainly the Information Technology Centre, Cyber Defence Operation Centre, Cyber Defence Branch and Electronic Warfare Regiment which are under the Defence Intelligence Staff Division as well as Armed Forces Crypto Team which further divided into each services (Army, Navy and Air Force) to tracked and summoned the personnel involves for further actions and have an equivalent punishment.

In the MAF itself, there are mainly two systems that are transmitting the secured information via closed-circuit network that make used of Internet Protocol Virtual Private Network (IPVPN) and encryption system which are first, Defence

Electronic Messaging System (DEMS) and second, Command and Control (C2) System. The signal transmission of the messages consist of information with pertinent level of security classification are relayed throughout the network hence requires the interconnected devices to allow the remote receivers and vice versa to dictate the real-time source and destination of the messages' owner as well as to ensure the speed of message delivery. Particularly, every information in the Armed Forces with security classification such as email transmission between strategic management, secure communication via secured phone, data operation communication via computerisation and video conferencing in the management have to be transferred and communicate securely. However, due to the limited interviewees' samples in the preliminary investigation, the SLR is conducted to have more significance idea on the topic conducted which the main concerned is to identify the factors of data leakage in the use of social media attributes practices in other fields which is then being mapped into the Armed Forces settings.

The MAF has its Network Centric Operation that has been recently introduced in January, 2015 with the spectrum carrier of X-Band above the usage of C-Band and K-Band that still operated in several places in the MAF. The newly introduce technology of X-Band is mainly reserved for the government agencies as well as for the military. The X-Band owned by the MAF is used to communicate with the satellite which is known as MEASAT-3b in the encrypted form that has four transponders which enable the information being transmitted from the sender to the receiver that affirms the improvements in efficiencies transmission of intelligence between units during a military operation.

3.3.2 Structured Literature Review

This research used the SLR in conducting the review of the literature in which suggested by Okoli and Schabram (2010). It assists in identifying, evaluating and synthesising the work of extant researchers, scholars and practitioners that is described as a systematic, explicit and reproducible method. It is being practised in order to find common and valuable attributes to be preserve as the model

construction. The steps identified in conducting this SLR is adopted from the Okoli and Schabram (2010) and Kitchenham and Charters (2007) that have introduced the SLR guidelines for the information system field which are categorised into planning of the review, execution of the review and writing the review phases which has been explain detailed in chapter 2.6.

3.4 Phase 2: Design

There are two parts involved in this phase in which the first part presented the development of the proposed conceptual model of factors influencing data leakage in the use of social media which are constructed based on the results of the SLR in the previous phase. The second part is followed by continuing with the questionnaire development based on the attributes findings in the literature review that consist of four attributes altogether.

3.4.1 Chosen Methodology

Factors influencing data leakage in the use of social media is much related to the personnel perception on the way of how the personnel look into the handling the perspectives they are facing. Many authors measure the perception of the personnel by conducting the questionnaire survey method (Baird, 2015;Mo *et al.*, 2015). Therefore, this research used the quantitative method with the development of the questionnaire structure to identify the factors influencing data leakage in the use of social media in the selected environment. It is to provide a self-determining and neutral evaluation of how the personnel grasp the practises of their daily routine in handling confidential data. In pursuance, a set of questions are established that reflect the factors influencing data leakage in the use of social media that are determined in the chapter of Literature Review.

3.4.2 Questionnaire Design

In this stage, the set of questionnaires related with the data leakage are designed in which the constructs are making use of the extracted attributes findings from the Literature Review chapter which consist of the SLR's results and related statement and the available questionnaires used by other researchers together with other researchers' statements to accommodate the development of the questionnaire in an effort to ensure that the questionnaires being delivered are acceptable to the respondents.

By doing these, the set of initial questionnaires are developed to ensure the suitability and connectivity of the questions with the environment setting. This questionnaire-based approach is intended to find out how the Armed Forces personnel reflected by selecting the population grasp each of the constructs in terms of attributes identified which has composed the data leakage conceptual model in in the use of social media. It will be distributed to the targeted respondents of 200 personnel based on the convenience sampling identified in the next phase.

The questionnaire structure for pilot study is based on the proposed conceptual model as attached in Appendix D that make used of Zimmer *et al.* (2010) literature ideas on questionnaire development structure for this research questionnaire development. It uses the construct of independent variables (IV) identified in related questions of the data leakage along with statements regarding the use of social media to be presented to the Armed Forces personnel in examining how the practised is in the environment.

As such, the compliment of the IV is the dependent variable (DV). IV in this research consists of the variable of Computer Usage Behavior, Security Awareness, Policy Acceptance & Understanding, Security Education & Knowledge while DV reflected the variable of Data leakage factors. The variables involved are depicted as in Table 3.2 in which the design of the questionnaire was based on.

Table 3.2: Proposed Conceptual Model for Data Leakage Model in The Use of Social Media

Variable	Type of Variable
Computer Usage Behavior	Independent Variable (IV)
Security Awareness	Independent Variable (IV)
Policy Acceptance & Understanding	Independent Variable (IV)
Security Education & Knowledge	Independent Variable (IV)
Data Leakage Factors	Dependent Variable (DV)

The questionnaire design structure consists of ten sections starting with section A on the respondents' profile where the questionnaire began, followed by section B on Computer Usage Behavior, section C on Security Awareness, section D on Policy Acceptance & Understanding, section E on Security Education & Knowledge, and section F on Data leakage factors. Five point Likert Scale will be used from section B until section F which denotes "strongly disagree" for Scale 1 and "strongly agree" for Scale 5.

3.5 Phase 3: Implementation

In this phase, there are several steps involving the population and sample design, formulating the questionnaires. Pilot study was conducted to revise the questionnaire and to distribute the corrected version of the questionnaire. The correct questionnaire will be distributed to the respondents identified at this stage.

3.5.1 Research Population and Sample

In determining the design population and sample, a convenience sampling technique is used by dividing the entire population in the identified scope which is the selected Armed Forces personnel into three different subgroups. However, in

this research only two subgroups are taken as the sample size. Convenience sampling is chosen because of the availability and easy approach (Sedgwick, 2013) to the selected personnel in the selected environment in which data can be gathered in quickest period as possible. The disadvantage of using this type of sampling is the risk that the sample might not represent the population as a whole which result to bias. It has been overcome as the reason stated later in this section.

Table 3.3 shows the population based on the categorised rank in the selected personnel of the MAF that consist the number of 97 NCO's personnel that constitutes 60 personnel of NCO's Senior Rank and 37 personnel of NCO's Junior Rank while for officers there are 90 personnel in total.

Table 3.3: Population Size of Selected MAF Personnel Categorised by Rank

No.	Respondents (Rank Category)	Number of personnel
1	Officers	90
2	NCO's Senior Rank	60
3	NCO's Junior Rank	37
	Total	187

The personnel identified are accordance to the selected population personnel in Malaysian Armed which involved NCO personnel from Sergeant, Staff Sergeant, Warrant Officer Class II, and Warrant Officer Class I in rank which is categorised as NCO's Senior Rank and Officers of Second Lieutenant, Lieutenant, Captain and Major in rank. Thus, the total number of questionnaire to be distributed is 187personnel.

3.5.2 Pilot Study

Before the actual questionnaire distribution, a pilot study is performed thus enable the questionnaire to be reviewed by experts as well as non-expert in the field in order to structure, organise and confirm the suitability of the questionnaire before

distributing it to the respondents. This process is done by distributing the preliminary questionnaire to the subject matter experts in data leakage that involves lecturers and senior defence administration in the Armed Forces that deals with every day confidential information handling as well as to the group of non-expert personnel to better know the levels of questions adaptation.

At this stage, 20 questionnaires were distributed among respondents. The questionnaires collected are then revised to be amended with regards of grammatical errors, enhancement of the questionnaires structured, suitability and sensitivity of the questions constructed, additional questions to be emphasised or any other alteration suitability. By doing this, the relevancy of the questionnaires towards the research objectives will be achieved.

3.5.3 Actual Survey

The actual survey stage is conducted after the questionnaires have gone through the stage of pilot study where it is executed after the latest version of the questionnaires has been finalised. The finalised questionnaire are distributed to the specified population that are gathered from the stage of population and sampling by which the distribution involved the personnel with accordance to the rank categories resulting from the convenience sampling that used the actual number of personnel that currently served in the selected population. Table 3.4 depicted the population size of the distribution of the actual survey.

Table 3.4: Population Size of Actual Survey Distribution

No.	Respondents (Rank Category)	Number of personnel
1	Officers	90
2	NCO’s Senior Rank	60
3	NCO’s Junior Rank	37
	Total	187

3.6 Phase 4: Analysis

This phase involves the evaluation of the questionnaire data collected in the previous phase of implementation. It involves the data to be screened at the first place to enable it to be gathered using the statistical analysis tool of SPSS version 20. It is to help in analysing and validating the gathered data. Throughout the analysis, the answers from the respondents are evaluated and that the relevancy of the developed model is measured using the analysis method available in the chosen statistical analysis tool.

3.7 Phase 5: Report Writing

All findings and related discovery from the first phase of information gathering and project planning up until the stage of analysis are documented. It served as a complete report that portrayed the research project fulfilment. It also indicates the achievement of the research objectives along with activities involved in each phase that comprises of respective stages together with the deliverable of the research for the whole research development. Altogether, there are five chapters involved in this research which are the chapter of Introduction, Literature Review, Research Methodology, Finding and Analysis followed by the last chapter which is the Discussion and Conclusion.

3.8 Research Deliverable

This research has its own milestone which is measured from research deliverable. Overall, there are three achievement portrayed in this section. Table 3.5 describes the summary of research deliverables that involves research questions, research objectives, activities and deliverables resulted in this research. It can be seen that the first achievement of the factors influencing data leakage in the use of social media is identified through SLR conducted which answered the research's

first objective. It is followed by the second achievement of the proposed conceptual model designed through the process of conducting literature review and consecutively mapped to the SLR's outcome which has answered the research's second objective. Last but not least, the third achievement of evaluated proposed conceptual model through the questionnaire distribution and findings interpretation made has answered the research's third objective.

Table 3.5: Summary of Research Deliverable

No	Research Question	Research Objective	Activities	Deliverables
1.	What is a security issue related to data leakage in the use of social media among Malaysian Armed Forces personnel	To identify security issue related to data leakage in the use of social media among Malaysian Armed Forces personnel	Literature Review: To identify security issue related to data leakage in the use of social media.	They related to data leakage factors in the use of social media are identified.
2.	How to model the factors of data leakage in the use of social media among Malaysian Armed Forces personnel?	To propose and design a model data leakage in the use of social media among Malaysian Armed Forces personnel?	Design a model of data leakage in the use of social media among Malaysian Armed Forces personnel based on literature review.	A propose model of data leakage in the use of social media was designed.
3.	How to evaluate the propose model of data leakage in the use of social media among Malaysian Armed Forces personnel organization	To evaluate the propose model of data leakage in the use of social media among Malaysian Armed Forces personnel	Design the questionnaire Pilot study Conduct surveys & distribute. Questionnaire analysis using SPSS Interview	Questionnaire booklet. Tested the reliability of the questionnaire. Questionnaire collected. Result of data analysis. Result of interview

3.9 Summary

The selective method to design this research is a quantitative research design. There are five phases in the development of this research which are information gathering and project planning phase which involved two main activities of: First, the preliminary investigation which involve literature review on related topics as well as preliminary interviewed to be conducted as to study on current data leakage in the MAF, second, conducting the SLR to identify the attributes of data leakage involved in other fields which to be measured in the Armed Forces. Next, the design phase involved the construction of the data leakage conceptual model based on findings acquired in SLR stage which then followed by the development of questionnaire. The implementation phase in which the identification of population and sample is determined based on Convenience Sampling technique while the reliability and suitability of the questionnaire to be distributed is being assessed by conducting a pilot study before distributing the corrected version of questionnaire. After that, the analysis phase is conducted which involves activities of screen and analyses the gathered data from the questionnaire distribution and followed by the last phase which is report writing that documented all the research findings. Next would be the Finding and Analysis chapter in which the findings will be documented and evaluated.

CHAPTER 4

FINDINGS AND ANALYSIS

4.1 Introduction

This chapter discusses the findings based on the research question. The main focus of the study focused on data from the questionnaire. Discussions of the findings for each research question are also discussed. At the end of this chapter, the researcher will conclude that the overall results obtained in this study.

4.2 Reliability

Reliability is an important aspect of research. This is to show to what extent these findings reflect the situation accurately studied. The concept of measurement reliability in quantitative methods, especially the use of a questionnaire designed to test the questionnaire through pilot (test pilots). This pilot study represents a beginning of trial (preliminary trial) before the items of the actual test applied to real samples. The purpose of the pilot study is to gain transparency of data from the trial by a small group of individuals.

The most researchers using Cronbach's Coefficient Alpha (α) to measure the reliability of the questionnaire items. The higher the degree of reliability of the instrument, the more accurate the data will be obtained to produce good-quality studies. Cronbach’s alpha is the tool to investigate the internal consistency (i.e. reliability) of the measures, and Cronbach’s alpha reliability coefficient normally

ranges between 0 and 1. According to Sekaran&Bougie (2012), the closer the reliability coefficient gets to 1.00 the better. They further proposed that reliability less than 0.6 are considered to be poor. Those in the range 0.6, acceptable and those over 0.8 is good.

Table 4.1: Test of Reliability

Factor	Cronbatch Alpha	No of Items
Computer Usage Behaviour	0.654	6
Security Awareness	0.712	6
Policy Acceptance & Understanding	0.601	6
Security Education & Knowledge	0.641	6
Data Leakage Factors	0.628	6

4.3 Face Validity

It is important to bear in mind that validity are not an all or none issue but a matter of degree. Validity is the extent to which a test measures what it is supposed to measure. The question of validity is raised in the context of the three points made above, the form of the test, the purpose of the test and the population for whom it is intended. Therefore, the question to ask is "how valid is this test for the decision that I need to make?" or "how valid is the interpretation I propose for the test?" We can divide the types of validity into logical and empirical. Basically face validity refers to the degree to which a test appears to measure what it purports to measure. According to Cronbach, to the question "what is a good validity coefficient?" the only sensible answer is "the best you can get", and it is unusual for a validity coefficient to rise above 0.60, though that is far from perfect prediction.From this research as shown as Table 4.1, all the attribute is above 0.6 and it is valid.

In this study, 10 respondents were used in the pilot study. As seen in Table 4.1, all factors showed the result was acceptable. The computer usage showed the Cronbatch's alpha is 0.654, security awareness is 0.712, policy acceptance and understanding is 0.601, and security education and knowledge is 0.641.While the Data Leakage Factors showed the Cronbatch Alpha is 0.628. Every questionnaire

items is said to be valid because the Cronbatch's alpha greater than 6. So, the data in this study can be classified as acceptable and adequate for this research means.

4.4 Normality Test

In statistics, normality test are used to determine if a data set is well-modelled by a normal distribution and to compute how likely it is for a random variable underlying the data set to be normally distributed. Normality is an important concept in statistics because before start the analyses, the researcher should check a dataset for normality before performing an analysis that relies on normally distributes data. When the data is normal, the test should be conducted using parametric but when the data is not normal, the non parametric test is used.

Based on Table 4.2, that all factors have a mean and median are very similar and based on the test of significantly found that each factor showed significant level of $p < 0.05$. This showed that it is not normal distribution and is suitable for further analysed for this study.This means that the test should be conducted using non parametric although all items are shaped Likert scale.

Table 4.2: Test of Normality for Each Factor

Factor	Mean	Median	SD	Skewness	P-value
Computer Usage Behaviour	3.751	3.833	0.432	-0.787	0
Security Awareness	3.021	3	0.558	-0.285	0
Policy Acceptance & Understanding	3.834	3.833	0.506	-0.818	0
Security Education & Knowledge	4.257	4.333	0.708	-0.989	0
Data Leakage Factors	3.741	3.667	0.473	-0.813	0

4.5 Descriptive Statistics

Descriptive statistics are used to explore the data collected and to summarize and describe those data (table, figure, frequency, percentage, mean and standard deviation). Descriptive statistics may be particularly useful if one just wants to make some general observations about the data collected.

4.5.1 Respondent Demographic

Dataofthe respondent's background consist by gender, service rank, work experience, education background, sharing confidential information and updating status using social media. There were 187 respondents from 200. The total numbers of samples involved in this study wereabout 187 people.

Table 4.3: Number of Respondents based on Gender

Gender	Frequency	Percent
Male	114	61
Female	73	39
Total	187	100

Based on Table 4.3, we conclude that a total of 114 peopleor 61% aremaleinvolved inthisstudyanda total of 73 people or39% are females. This show the respondent by male is higher than female.

Table 4.4: Number of Respondents based on Service Rank

Service Rank	Frequency	Percent
Prebat/LansKoperal/Koperal	37	19.8
Sarjan/Staff Sarjan/ Warrant Officer Class II/ Warrant Officer Class I	60	32.1
Second Lieutenant/Lieutenant/Captain/Major	90	48.1
Total	187	100

Based on Table 4.4, the findings shown the service rank of respondents. Based on the data obtained, there were 37 people or 19.8% are from Prebat/LansKoperal/Koperal. This was followed by Sarjan/ Staff Sarjan/ Warrant Office Class II/Warrant office Class II by 60 people or 32.1%. Then, the respondents also Second Lieutenant/ Lieutenant/ Captain/ Major by 90 people or 48.1%. Thisrepresented the highest number of respondents who are and the lowest are Prebat/LansKoperal/Koperal.

Table 4.5 below show the number of respondents based on work experience. Based on the data obtained, there have 48 people or 25.7% for the less than 6 year experience. This was followed by 17 people or 9.1% of respondents had 6 to 10 years and 75 people or 40.1% of respondents had 11 to 15 years. Besides that, the respondents who had more than 15 years were 47 people or 25.1%. This representedthe highest numberof respondents for the respondent work experience between 11 until 15years and the lowest are between 6 until 10 years.

Table 4.5: Number of Respondents based on Experience

Work Experience	Frequency	Percent
< 6 years	48	25.7
6 - 10 years	17	9.1
11 - 15 years	75	40.1
> 15 years	47	25.1
Total	187	100

Based on the Table 4.6 below, the findingsshow the level of education of respondents. Based onthe data obtained, there were 1 people or 0.5% are master degree. This was followedby 85 people or 45.5%of people had Bachelor's Degree.While for respondents who had Diploma were 10 people or 5.3% and SPM were 81 people or 43.3%. Then the respondents who had PMR were 10 or 5.3%.This represented the highest number of respondents whohavebeen Bachelor's Degree and the lowest are Master's Degree.

Table 4.6: Number of Respondents based on Education Level

Education Background	Frequency	Percent
Master Degree's	1	0.5
Bachelor Degree's	85	45.5
Diploma	10	5.3
SPM	81	43.3
PMR	10	5.3
Total	187	100

Based on the Table 4.7 below, the findingsshowed the sharing confidential information in social media aware. 152 or 81.3%. Based on the result showed, the students aware about sharing confidential information in social media will cause of data leakage were 152 or 81.3%. Then the students also not aware about that were 9 people or 4.8% and not sure showed 26 people or 13.9%.

Table 4.7: Number of Respondents based on Sharing Confidential Information

Are you aware that sharing confidential information in social media will cause of data leakage?	Frequency	Percent
Yes	152	81.3
No	9	4.8
Not Sure	26	13.9
Total	178	100

Based on the Table 4.8 below, the findingsshow the frequently updating status using social media. Based on the result showed, the students frequently updating status using social media were 114 people or 61% and followed by no frequently update were 45 people or 24.1% and not sure about that showed 28 people or 15%.

Table 4.8: Number of Respondents based on Updating Status Using Social Media

Are you frequently updating your status using social media?	Frequency	Percent
Yes	114	61
No	45	24.1
Not Sure	28	15
Total	187	100

4.5.2 To Identify The Data Leakage Attributes.

There are four factors influencing data leakage attributes. There are computer usage behaviour, security awareness, policy acceptance and understanding and security education and knowledge.

4.5.2.1 Computer Usage Behaviour

Table 4.9 represents the frequencies and percentages for computer usage behaviour. As shown in Table 4.9, a substantial majority of the respondents chooses strongly agree about *"I will make sure my computer was turn off before I leaving my workstation"*(48.7%) and followed agree by *"I think about the social consequences of the confidential information that I wrote in social media"(*42.2%). However, the respondents also disagree about *"I will use my friend's password to access other system that I am not authorized for"*. The respondents also neutral about *"I do not use other personal computer resources without authorization to conserve the confidential information that may exist in it"* (16%). As seen in Table 4.9, the respondents showed various reactions towards the computer usage behaviour. The respondents agree about *"I will make sure my computer was turn off before I leaving my workstation" (*with a mean of 4.262, SD=0.88).The overall mean computer usage behaviour is 3.75 and standard deviation is 0.432. These shown the respondents neutral about computer usage behaviour.

Table 4.9: Frequencies And Percentages of Computer Usage Behaviour

Statement	1	2	3	4	5	Mean	SD
I will make sure my computer was turn off before I leaving my workstation	3 (1.6%)	3 (1.6%)	27 (14.4%)	63 (33.7%)	91 (48.7%)	4.262	0.88
I will use my friend's password to access other system that I am not authorized for	55 (29.4%)	75 (40.1%)	26 (13.9%)	28 (15%)	3 (1.6%)	2.195	1.07
I will always keep my email account in sign in mode to simple get the email update	13 (7%)	27 (14.4%)	29 (15.5%)	76 (40.6%)	42 (22.5%)	3.572	1.186
I will make sure my selecting password is strong enough using combination of symbol and alphabet	2 (1.1%)	5 (2.7%)	28 (15%)	74 (39.6%)	78 (41.7%)	4.181	0.86
I think about the social consequences of the confidential information that I wrote in social media	1 (0.5%)	5 (2.7%)	29 (15.5%)	79 (42.2%)	73 (39%)	4.165	0.822
I do not use other personal computer resources without authorization to conserve the confidential information that may exist in it	3 (91.6%)	7 (3.7%)	30 (16%)	69 (36.9%)	78 (41.7%)	4.133	0.926

4.5.2.2 Security Awareness

Table 4.10 represents the frequencies and percentages for security awareness. As shown in Table 4.10, a substantial majority of the respondents chooses strongly disagree about *"I will write down my computer password and share with my friend"* (47.1%). However, the respondents also strongly agree about *"I routinely doing frequent virus update and scanning on my computer* and followed by "I believe confidential information should be treated equally due to the provision of accessibility right" and *"I will allow my staff using my personal computer when I am on leave"*(39%).As seen in Table 4.10, the respondents showed various reactions towards security awareness. The respondents neutral about *"I routinely doing frequent virus update and scanning on my computer" (*with a mean of 4.053, SD=1.061).The overall mean security awarenessis 3.021 and standard deviation is 0.558. These shown the respondents neutral about security awareness.

Table 4.10: Frequencies And Percentages of Security Awareness

Statement	1	2	3	4	5	Mean	SD
I routinely doing frequent virus update and scanning on my computer	5 (2.7%)	11 (5.9%)	37 (19.8%)	50 (26.7%)	84 (44.9%)	4.053	1.061
I allow my web browser to accept cookies from web site	54 (28.9%)	61 (32.6%)	31 (16.6%)	36 (19.3%)	5 (2.7%)	2.342	1.164
I am using an official email to send sensitive data outside the organization	10 (5.3%)	24 (12.8%)	33 (17.6%)	50 (26.7%)	70 (37.4%)	3.78	1.226
I will allow my staff using my personal computer when I am on leave	6 (3.2%)	19 (10.2%)	35 (18.7%)	54 (28.9%)	73 (39%)	2.09	1.105
I will write down my computer password and share with my friend	88 (47.1%)	49 (26.2%)	24 (12.8%)	22 (11.8%)	4 (2.1%)	1.957	1.125
I believe confidential informationshould be treated equally due to the provision of accessibility right	6 93.2%)	19 (10.2%)	35 (18.7%)	54 (28.9%)	73 (39%)	3.903	1.127

4.5.2.3 Policy Acceptance and Understanding

Table 4.11 represents the frequencies and percentages for policy acceptance and understanding. As shown in Table 4.11, a substantial majority of the respondents chooses agree about *"I believe policy acceptance and understanding is important to prevent adapt leakage in the use of social media"* (49.7%) and followed by *"I will comply with the data security policy while performing my duties"* (48.1%). However, the respondents also disagree about *"I confused with the policy and did not understand well"*(29.4%). As seen in Table 4.11, the respondents showed various reactions towards the policy acceptance and understanding. The respondents neutral about *"I know that MAF has a policy that specify they do and don't relate to ICT" (*with a mean of 4.192, SD=0.907).The overall mean policy acceptance and understanding is 3.8342 and standard deviation is 0.506. These shown the respondents neutral about policy acceptance and understanding.

Table 4.11: Frequencies And Percentages of Policy Acceptance and Understanding

Statement	1	2	3	4	5	Mean	SD
I know that MAF has a policy that specify they do and don't relate to ICT	4 (2.1%)	7 (3.7%)	17 (9.1%)	80 (42.8%)	79 (42.2%)	4.192	0.907
I believe the ICT policy in MAF was a comprehensive guideline for staff	1 (0.5%)	7 (3.7%)	25 (13.4%)	88 (47.1%)	66 (35.35)	4.128	0.819
I will comply with the data security policy while performing my duties	0 (0%)	4 (2.1%)	26 (13.9%)	90 (48.1%)	67 (35.8%)	4.176	0.744
I fully understood by the policy and refer to the policy while when facing a problem.	2 (1.1%)	7 (3.7%)	39 (20.9%)	85 (45.5%)	54 (28.9%)	3.973	0.864
I believe policy acceptance and understanding is important to prevent adapt leakage in the use of social media	2 (1.1%)	4 (2.1%)	21 (11.2%)	93 (49.7%)	67 (35.8%)	4.171	0.791
I confused with the policy and did not understand well	54 (28%)	55 (29.4%)	43 (23%)	26 (13.9%)	9 (4.8%)	2.363	1.176

4.5.2.4 Security Education and Knowledge

Table 4.12 represents the frequencies and percentages for security education and knowledge. As shown in Table 4.12, a substantial majority of the respondents chooses strongly agree about *"I agree that my agency needs a data security policy in ICT" (*52.9%) and followed by *"I believe security education is important for all the staff that handling confidential information*(49.7%). However, the respondents disagree about *"I fully understood with the policy and procedure in my organization"* (3.7%). There are neutral about *"I fully understood with the policy and procedure in my organization"*(18.7%). As seen in Table 4.12, the respondents showed various reactions towards the security education and knowledge. The respondents agree about *"I agree that my agency needs a data security policy in ICT" (*with a mean of4.347, SD=0.817).The overall mean security education and knowledge is 4.257and standard deviation is 0.708. These shown the respondents agree about security education and knowledge.

Table 4.12: Frequencies And Percentages of Security Education and Knowledge

Statement	1	2	3	4	5	Mean	SD
I believe security education is important for all the staff that handling confidential information	2 (1.1%)	5 (2.7%)	25 (13.4%)	62 (33.2%)	93 (49.7%)	4.278	0.872
I agree that my agency needs a data security policy in ICT	1 90.5%)	4 (2.1%)	23 (12.3%)	60 (32.1%)	99 (52.9%)	4.347	0.817
I fully understood with the policy and procedure in my organization	2 (1.1%)	7 (3.7%)	35 (18.7%)	61 (32.6%)	82 (43.9%)	4.144	0.924
I agree that educating staff through a security campaign is beneficial	1 (0.5%)	5 (2.7%)	24 (12.8%)	77 (41.2%)	80 (42.8%)	4.229	0.813
I am aware that discrimination of military information which is clarified as confidential not to hare in social media	2 (1.1%)	1 (0.5%)	20 (0.7%)	78 (41.7%)	86 (46%)	4.31	0.769
I believe training on data security in my organization is important to all staff	0 (0%)	6 (3.2%)	21 (11.2%)	83 (44.4%)	77 (41.2%)	4.235	0.774

4.5.3 To Identify The Most Data Leakage Attributes

Table 4.13 represents the overall data leakage attributes. As shown in Table 4.13, the security education and knowledge showed the mean were 4.257 and standard deviations were 0.708. There is the first rank from the other factors. This showed the respondents choose the factor as the best factor influencing data leakage attributes. Then, the second ranks were policy and acceptance and understanding with mean 3.834 and the standard deviation was 0.506. Then the third ranks were computer usage behaviour with mean 3.751and standard deviation was 0.432. Next, the industrial relation are forth rank with mean 3.47 and the standard deviation are 0.725 and the fifth rank are job security with mean 3.39 and standard deviation are 0.701.While the last rank are security awareness with mean 3.021 and standard deviation are 0.558.

Table 4.13: Rank of Factor

Factor	Mean	SD	Rank
Computer Usage Behaviour	3.751	0.432	3
Security Awareness	3.021	0.558	4
Policy Acceptance & Understanding	3.834	0.506	2
Security Education & Knowledge	4.257	0.708	1

4.5.4 To Describe The Data Leakage Factors

Table 4.14 represents the frequencies and percentages for Data Leakage Factors. As shown in Table 4.14, a substantial majority of the respondents chooses strongly agree about *"The employee should give an opportunity to attend any professional certification to improve their knowledge and understanding*" (44.9%). It was followed agree about *"The understanding on security policy and procedure govern in organization will reduce the security breach and dataleakage"* (42.2%). However, the respondents also disagreeabout *"Top management contribution was needed to enforce the security practice in organization"*(32.6%). As seen in Table 4.14, the respondents showed various reactions towards the Data Leakage Factors. The respondents agree about *"Security Technology is the first lines of defense in organizational towards Data Leakage Factors" (*with a mean of 4.181, SD=0.86).The overall mean Data Leakage Factors is 3.741 and standard deviation is 0.473. These shown the respondents neutral about Data Leakage Factors.

Table 4.14: Frequencies And Percentages of Data Leakage Factors

Statements	1	2	3	4	5	Mean	SD
Human awareness is the first lines of defense in organization towards information leakage prevention	13 (7%)	27 (14.4%)	29 (15.5%)	76 (40.6%)	42 (22.5%)	3.572	1.186
Security Technology is the first lines of defense in organizational towards data leakage factors	2 (1.1%)	5 (2.7%)	28 (15%)	74 (39.6%)	78 (41.7%)	4.181	0.86
The understanding on security policy and procedure govern in the organization will reduce the security breach and information leakage	1 (0.5%)	5 (2.7%)	29 (15.5%)	79 (42.2%)	73 (39%)	4.165	0.822
Security training and education program should be done periodically	3 (1.6%)	7 (3.7%)	30 (16%)	69 (36.9%)	78 (41.7%)	4.133	0.926
The employees should given an opportunity to attend any professional certification to improve their knowledge and understanding	5 (2.7%)	11 (5.9%)	37 (19.8%)	50 (26.7%)	84 (44.9%)	4.053	1.061
Top management contribution was needed to enforce the security practice in organization	54 (28.9%)	61 (32.6%)	31 (16.6%)	36 (19.3%)	5 (2.7%)	2.342	1.164

4.6 Statistical Test

Inferential statistic is statistic used to describe relationship between the variables. In this research, correlation and regression test are used to determine the relationship between the variable.

4.6.1 Correlation

As this is a correlation study, the results report Pearson correlation coefficients as a measure of the linear relationships that exist among the Data Leakage Factors with computer usage behaviour, security awareness, policy acceptance and understanding and security education and knowledge. The range of

the correlation coefficient is from –1 to +1. If there is a strong positive linear relationship between the variables the value of r will be close to +1. If there is a strong negative linear relationship between the variables the value of r will be close to -1. When there is no linear relationship between the variables or only a weak relationship, the value of r will be close to 0.

The findings provide insights into the hypotheses of this study:

H_0: There is no relationship between independent variable (computer usage behaviour, security awareness, policy acceptance and understanding and security education and knowledge) with dependent variable (Data Leakage Factors).

H_1: There is relationship between independent variable (computer usage behaviour, security awareness, policy acceptance and understanding and security education and knowledge) with dependent variable (Data Leakage Factors).

This chapter begins with a description of each construct. It then moves to the statistical analyses of the relationships between these variables. Based on the results of the respondents survey and the relevant correlations found between it and the relationship was discovered. When assessing factors contributing to overall organization, the relationship described in table below has been made.

H1: There was a significant positive correlation between the behaviour of computer use and factors of data leakage in the use of social media.

Table 4.15 represents the factor correlation analysis reveals these results. Here, the result shows (r = 0.857 n=187 p=0.000). So, we can conclude that the behaviour of computer use and factors of data leakage were significantly positively correlated for respondents. Based on the P-value, there is a significant linear relationship between behaviour of computer use and factors of data leakage.

Table 4.15: The Relationship Behaviour Of Computer Use and Factors Of Data Leakage

Correlation			Significance
Behaviour of computer use	➡	Factors of data leakage	Significance p=0.000

H2: There was a significant positive correlation between education security and knowledge and factors of data leakage in the use of social media.

Table 4.16 represents the factor correlation analysis reveals these results. Here, the result shows (r = 0.531 n=187 p=0.000). So, we can conclude that the education security knowledge and factors of data leakage were significantly positively correlated for respondents. Based on the P-value, there is significant linear relationship between the education security and knowledge and factors of data leakage in the use of social media.

Table 4.16: The Relationship The Education Security and Knowledge And Factors of Data Leakage

Correlation			Significance
Education security and knowledge	➡	Factors of data leakage	Significance p=0.000

H3: There is a positive significant relationship between security awareness and factors of data leakage in the use of social media.

Table 4.17 represents the factor correlation analysis reveals these results. Here, the result shows (r = 0.357 n=187 p=0.000). So, we can conclude that the security awareness and factors of data leakage were significantly positively correlated for respondents. Based on the P-value, there is a significant linear relationship between security awareness and factors of data leakage.

Table 4.17: The Relationship The Security Awareness and Factors of Data Leakage

Correlation	Significance
Security Awareness ➡ Factors of data leakage	Significance p=0.000

H4: There is a positive significant relationship between policy acceptance and understanding and factors of data leakage in the use of social media

Table 4.18 represents the factor correlation analysis reveals these results. Here, the result shows (r = 0.572 n=187 p=0.000). So, we can conclude that the relationship with policy acceptance and understanding and factors of data leakage were significantly positively correlated for respondents. Based on the P-value, there is a significant linear relationship between the relationship with policy acceptance and understanding and factors of data leakage.

Table 4.18: The Relationship The Relationship With Policy Acceptance And Understanding and Factors of Data Leakage

Correlation	Significance
Policy Acceptance and Understanding ➡ Factors of data leakage	Significance p=0.000

In this first project, the proposed model is being derived by which the attributes identified will be measured in project 2 with the implementation of the questionnaire development that is to be developed based on the attributes. All of the attributes will be tested in the Armed Forces environment on selected population as discussed in Chapter 3 of Research Population and Sample Section in which extend the attributes of other fields of studies impacted the Armed Forces with the assumption that the sample population would reflects the whole organization. The findings of the questionnaire which is the data gathered will be analysed to get the actual results in answering the third research question of this research as well as identifying the conformance of the model from the actual surveyed being conducted. Finally, the actual model of data leakage factors in the use of social media will be derived to serve as the major contribution of this conducted research.

4.7 Conclusion

This chapter has covered the fourth phase of Research Operational Framework in which the analysis has been done by making used of several techniques offered in SPSS version 19 packages software. All the variables and items have been analysed starting with the demographic profile, variables and its respective items, followed by factor analysis which yield the new number of factors that emerged after several rotation, reliability, correlation and regression analysis. Based on the results, it can be observed that the new IVs of security awareness, policy acceptance and understanding, security education and knowledge. influence the DV of Data Leakage Factors. From the findings obtained in this chapter, it determined the success of the objectivity defined in the first chapter of this research and consecutively had answered the objectives of the attributes, model and analytical part of the model derivation.

CHAPTER 5

DISCUSSION AND CONCLUSION

5.1 Introduction

This chapter consists of five sections that will discuss and conclude this study. The first section consists of the research findings, followed by limitations and recommendations for future research. The next section describes on this study's contribution to the information security world and finally the conclusion is discussed on the overall processes and findings of this study.

5.2 Summary of the Research Finding

This research focuses on three main objectives which are: first, identifying the attributes of data leakage factors in the use of social media, followed by the second objective which is designing the factors of data leakage model in the use of social media and the third objective of evaluating the factors of data leakage model in the use of social media that has been designed in the selected environment of the Armed Forces. Overall, all of these three objectives have successfully been fulfilled which will be discussed further in the following sub section for each objective's findings.

5.2.1 Findings for First Objective : To Identify The Factors Of Data Leakage Attributes In The Use Of Social Media Among MAF Personnel

The first objective of "to identify the factors of data leakage attributes in the use of social media among MAF personnel" has been achieved by making used of Systematic Literature Review techniques which has been done during Information Gathering and Project Planning Phase. This SLR has been beneficiated from the exhaustive searches through seventeen related journals and hence, there are 4 attributes that are identified during the SLR stages. Among them are the computer usage behavior, security education and knowledge, security awareness and policy acceptance and understanding.

5.2.2 Findings for Second Objective : To Design The Data Leakage Model In The Use Of Social Media For The Armed Forces

The objective number two of this research which is "to design the data leakage model in the use of social media for the Armed Forces" remarks the right achievement when a total of nine attributes found during the SLR (achieved in first objective) have consecutively being mapped to the three models identified in the Literature Review. These steps had produced the proposed conceptual model for factors of data leakage which signifies the success of this second objective. Based on the proposed model that consist of four IVs and one DV, a set of questionnaires are developed, piloted and distributed to the selected population of MAF personnel which actively handles the confidential data and using the social media.

5.2.3 Findings for Third Objective : To Evaluate The Data Leakage Model In The Use Of Social Media For The Armed Forces

The third objective of this research is "to evaluate the data leakage model in the use of social media for the Armed Forces" which has been successfully implemented during the phase of Analysis. The proposed model identified in the second objective has been tested and evaluated by using several techniques offer in SPSS version 19 software such as descriptive analysis, reliability analysis, correlation analysis and regression analysis. From the findings, it has demonstrated that all four attributes in the proposed conceptual model of factors of data leakage model may significantly influence the factors of data leakage model in the use of social media for the Armed Forces. Hypothesises constructed for each attribute have been tested and evaluated according to their relationship which have returned the following summarised findings of:

i. H1: There was a significant positive correlation between the behavior of computer use and factors of data leakage in the use of social media.

ii. H2: There was a significant positive correlation between education security and knowledge and factors of data leakage in the use of social media.

iii. H3: There is a positive significant relationship between security awareness and factors of data leakage in the use of social media.

iv. H4: There is a positive significant relationship between policy acceptance and understanding and factors of data leakage in the use of social media

The analysis namely a correlation analysis has been conducted and in overall, it can be observed that all the newly emerged of this four hypothesis is were all supported. From the findings, it had also been strengthen by the results of the behavior of computer use (H1), education security and knowledge (H2), security awareness (H3), and policy acceptance and understanding (H4) have annotated that the attributes have a significant as well as a strong positive towards the factors of data leakage in the use of social media in the Armed Forces.

This study mainly focuses on identifying components that significantly influence the factors of data leakage. Besides, the study also attempts to find the relationships between each component towards factors of data leakage in the use of social media. The model of factors influencing data leakage in MAF was developed based on the results of the analysis. Based on objectives of this study, factors that influencing data leakage in MAF are identified and model for factors influencing data leakage in MAF was developed. The conceptual model for factors influencing data leakage in MAF has been clearly explained in the previous chapter. Figure 5.1 Summarizes the relationships between all variables.

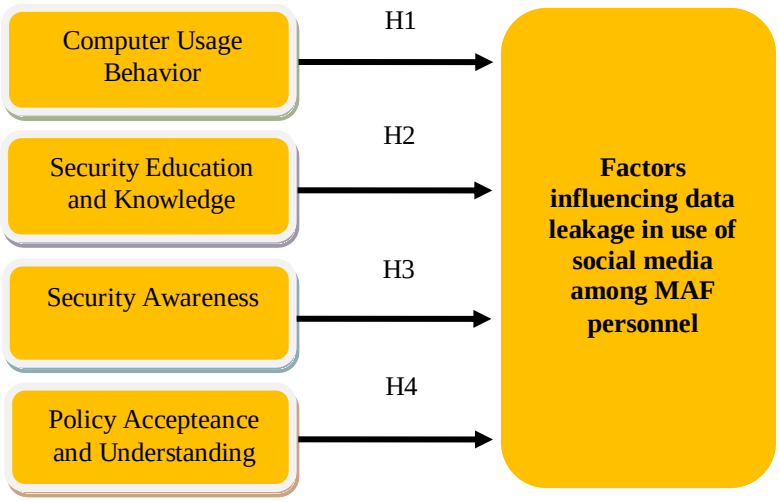


Figure 5.1 Summarises the relationships between all variables.

i. Computer Usage Behavior Components

Based on the results, it was determined that computer usage behavior has a positive and significant influence on the factors influencing data leakage in MAF personnel. This can be concluded that when computer usage behavior among employee increases, the factors influencing data leakage in MAF will also increase. This component could influence employee to be more cautious and be alert in their daily routine while using the computers. Therefore, this hypothesis is supported.

ii. Security Education and Knowledge Components

The findings have proven that there is a significant relationship between security education and knowledge and the factors influencing data leakage in MAF personnel. The positive relationship is proven when both the security education and knowledge and factors influencing data leakage in MAF increase in unison. Thus, this hypothesis is supported. In addition, when the employees have sound education and knowledge on security, they would likely to know what action and decision to take when an incident occurs hence they will be more aware and responsive towards preventing the organization's information from any means of destruction.

iii. Security Awareness Components

The findings indicated that security awareness has a strong influence on the factors influencing data leakage in MAF personnel. This positive relationship shows that increased level of security awareness will impact factors influencing data leakage in MAF positively. Based on the results, it also shows that the security awareness could influence the employee to better understand the importance of information security. Hence, this hypothesis is supported.

iv. Policy Acceptance and Understanding

Result of analysis shows that this hypothesis is supported, influence of policy acceptance and understanding is significantly influencing the factors influencing data leakage in MAF personnel. Hence, this hypothesis is supported.

5.3 Recommendations

Rapid technology advancement and social media has undeniably assist personnel in many walks of life. It is due to the universal access to the data that is largely stored in digital environment. The case has upsurges pressures to the MAF organisation in overcoming problems that may arise while appreciating the pros that

technology and social media could brings, and at the same time struggling to protect the safety and national defence. The social media used need to be free from any mishandling of confidential data to evade threats and information dissemination. From this phenomenon, along the confidential data handling are much required since human discourse will reflects between ethical and unethical judgment of the social media used which might contaminate the confidential data. This research has identified a total of four attributes that may influence the factors of data leakage in the use of social media for the Armed Forces environment.

From the results obtained via regression analysis, the regression values in variables for Accuracy having the highest regression value, all are of significant with moderate to strong positive relationship between each IV towards a DV as in the results derived from the correlation analysis. Thus, all these variables can be proposed to the Armed Forces to give greater emphasis a data from being leaked in the use of social media.

5.4 Limitation of the Research

The model developed is accordance to only the findings from conducting exhaustive searches in SLR mainly in four selected databases and also accordance to the selected field in Digital Library, ScienceDirect, and Taylor & Francis Online.

This has brought to the first limitation, that the results are confined to only four identified attributes of data leakage factors to be reviewed throughout the research as there might be other attributes that might fill in the residual percentage of predictors gathered during regression test that might significantly influence the factors of data leakage in the use of social media for the Armed Forces. It is attributable to scarce resources and time constraints.

On the other hand, the second limitation is, the population selected is only limited to a small organisation of 900 personnel although the sample size usage is in

the exact figure. The data collected will be more enhanced if all population is selected to be respondents or by using stratified sampling technique by using sample size table introduced by Krejcie and Morgan (1970) for the total number of population of 900 instead of 187 respondents. The selected organisation of MAF personnel has represented the whole population of the Armed Forces that is known to actively deal with confidential data and social media and thus the findings are more towards the point of view of the selected environment.

5.5 Recomendation For Future Research

Any other research will always be an enhancement for the current findings. Hence, this research on factors of data leakage in the use of social media for the Armed Forces can be enhanced in order to get versatility as well as finer results in future. The enhancement for this research can be done by:

i. Selecting a larger sample size such as based on specific rank categories of the specific Corp or service line. It will yield in more accurate finding results.

ii. Including more unit of analysis such as population that involve combination of all service rank on specific Corp or combination of specific service rank.

iii. Conducting comprehensive analysis for more library databases and widen the field on other attributes for factors of data leakage not considered in this research to be tested in the selected environment. These would contribute in finding the unexplained attributes as predictors that determine the predicted data leakage in the use of social media for the Armed Forces in this research which has been observed in regression test or even conveys in finding the greater influencer if any.

iv. Applying the model to other government, public as well as private organisations to have relative comparison on the data leakage attributes they may possess.

5.6 Research Contribution

This part converse the contribution of this research in data leakage factors perspective. Among others, this research has represented the first recorded research in data leakage factors in the use of social media whereby the setting is Armed Forces. This research may help the personnel in the Armed Forces organisation in performing routine of handling the confidential data with adherence to the factors of data leakage attributes identified in this research. While confidential information requires special care in handling valuable assets owned by the organisation, this research can be served as a central point for future researchers in designing standard with regards to data leakage factors in future.

Furthermore, this research has discovered four factors of data leakage attributes which have influenced ultimately the Armed Forces personnel in handling confidential data and using social media. Finding indicates Accuracy plays vital role among personnel while performing duties for the task accomplishment. With these findings, it could manoeuvre the organisation to determine the most suitable training needed in improving personnel skills and knowledge to strengthen the accuracy commitment among personnel. Other than that, it could also assist the organisation in motivating personnel for example conducting the security awareness programs to understand and appreciate the identified attributes and consequently encourage them the best practices in realm routine.

5.6.1 Theoretical Contribution

The biggest contribution of this study is establishing a model for factors that influencing data leakage in use of social media among MAF personnel. This model can be used as a guide for MAF and government agencies to ensure that the data leakage can be controlled among employees. All factors have been identified in the context of strengthening security awareness with respect to current information security threats.

5.6.2 Methodological Contribution

The results of the survey show that it may be useful for the organization to conduct an assessment on security among their employees. It also can be used as a guideline for budget submission to the management in order to enhance security knowledge and awareness among employee. This research may be beneficial in measuring the level of security in the organization.

5.6.3 Practical Contribution

Data leakage is controlled with the emphasized use of technology without concern on other factor while human plays a very important role in ensuring the success of the technology used. So, this study has shown other factors that influence the success of technology by developing this Factors influencing data leakage in MAF Model. This result also requires management to give serious attention to the factors that have been identified in order to ensure the success in the data leakage prevention.

5.7 Conclusion

As a conclusion, factors that influencing data leakage in MAF have been identified. Computer usage behaviour, security education, knowledge and security awareness and policy acceptance and understanding influence significantly towards factors influencing data leakage in use of social media. This results show that unintentional threats can be monitored or mitigated by increasing employees' intrinsic motivation, providing proper trainings, implementing them with the high level of usability, adjusting time pressure and workload on employees, and lastly by increasing awareness among users and management (Yayla, 2011). A result shows that each employee in the organization should be sure of their responsibility in securing the information assets in the organization. Generating awareness among

employee requires understanding, acquiring skills, learning and using the knowledge of which the latter is critical to the success of the security awareness program. The level of success of the program is influenced by change in people's behavior. This is required to ensure positive changes in security culture within the organization. Therefore, organization must enforce computer security knowledge in order to build good computer usage behaviour and awareness among employee to ensure all security breach and threat will be prevented. Security Education Training and Awareness (SETA) should be strengthened among employee in the organization so that they will be more alert on the implications of the security breach. Employee should provide with internal training, courses or guideline book to establish their good security practice. In conclusion, it is imperative for organisations to ensure adequate participation of organisation officials in the implementation of information security controls throughout the organization. This would include sufficient harmonization of information security governance activities with the overall organizational structure. On the user's end, security tools such as anti-virus program, crypto software, firewalls and any other programmed procedures should be implemented to prevent the users from committing further security breaches thus create a safety environment for personal or working purpose.

REFERENCES

Ajzen, I. (1991). *The Theory of Planned Behaviour.OrganisationalBehaviour and Human Decision Process*, 50(2), 179- 211.

Alexa.(2011). Global top sites. From http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

BBC. (2010). Israeli military 'unfriends' soldier after Facebook leak from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: *An Empirical Study of Rationality-based Beliefs and Information Security Awareness*. MIS Quarterly, 34(3), 523-548.

Chang, S. H., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems.

Colwill, C. (2010). *Human factors in information security: The insider threat - Who can you trust these days?* Information Security Technical Report, in press.

Comerford, J. D. (2006). Competent computing: A lawyer's ethical duty to safeguard the confidentiality and integrity of client information stored on computers and computer networks. The Georgetown Journal of Legal Ethics

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI conference on Human Factors in Computing Systems.

Dhillon, G., &Torkzadeh, G. (2006).Valuefocused assessment of information system security in organizations. Information Systems Journal

Everett, C. (2010). *Social media: opportunity or risk?* Computer Fraud & Security, 8-10.

Gudaitis, T. (2010).*The Impact of Social Media on Corporate Security: What Every Company Needs to Know.* Cyveillance, Inc.

Herath, T., &Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems

Institute, S. (2007). *Data Leakage - Threats and Mitigation*.SANS Institute.

Knapp, K. N., Morris Jr., R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security.

Lean-ping, O., &Chien-fatt, C. (2014).*Information Security Awareness : An Application of Psychological Factors – A Study in Malaysia*, (Ccit).

McAfee. (2010). Protecting Your Critical Assets: Lessons Learned from "Operation Aurora": McAfee, Inc.

Moen, V., Klingsheim, A. N., Simonsen, K. F., & Hole, K. J. (2007).Vulnerabilities in egovernments.International Journal of Electronic Security and Digital Forensics.

Nor, F. M. F. (2014).*Factors Influencing Implementation Of Information Leakage Prevention For Government Sector.* Thesis Master of Science, UniversitiTeknologi Malaysia.

Paul, I. (2010). The Facebook data torrent debacle: Q&A. PCWorld.

Smith, A. M., &Toppel, N. Y. (2009*). Case study: Using security awareness to combat the advanced persistent threat*. Paper presented at the 13th Colloquium for Information Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle.

Solomon, M. G., &Chapple, M. (2005). Information Security Illuminated (Jones and Barlett Illuminated). Sudbury, MA: Jones and Bartlett Publishers, Inc

Sophos. (2010). Security Threat Report: 2010. Boston, Massachusetts: Sophos Group.

Straub, D. (1990). *Effective IS Security*. Information Systems Research, 1(3), 255-276.

Symantec. (2010). Symantec Global Internet Security Threat Report: Trends for 2009. California, U.S.: Symantec Corporation.

Theoharidou, M., Kokolakis, S., Karyda, M., &Kiountouzis, E. (2005). *The insider threat to information systems and the effectiveness of ISO17799*. Computers & Society 24, 472-484.

Titus. (2008). Best Practices for a Successful DLP Deployment.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476–486.

Westervelt, R. (2009). *Botnet masters turn to Google, social networks to avoid detection*.http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373974,00 .html

Wilson, J. (2009). *Social networking: the business case*. Engineering & Technology (4)10 54-56.

Workman, M., &Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58(2), 212-222.

Yayla, A. A. (2011). Controlling Insider Threats With Information Security Policies.

Young, K. (2010). *Policies and procedures to manage employee Internet abuse*. Computers in Human Behaviour, 26, 1467-1471.

Zafar, H. (2013). *Human resource information systems: Information security concerns for organizations*. Human Resource Management Review, 23(1), 105– 113.

Zakaria, N. H., &Katuk, N. (2013).*Towards designing effective security messages: Persuasive password guidelines*. 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), 2013, 129–134.

APPENDIX A

Interview Outline of preliminary interviews with Confidential Data Handling and Data Leakage Experienced Respondents

The purpose of this study is to gain a a better understanding on data leakage practices in the use of social media in MAF.

1. Military personnel who have experiance with the confidential data handling and monitoring a cases in social media.

Main Research Question:
What are the data leakage involve in the MAF?

List of Topics

a. General Information
b. Confidential Data in MAF
c. Directives involve in the Confidential data in the MAF
d. Security Mechanism
e. Training Involve
f. Responsibility of departments
g. Action taken in data leakage
h. Security Threats
i. Factors of data leakage

APPENDIX B

Advanced Informatics School (UTM AIS)

FACTORS INFLUENCING DATA LEAKAGE IN USE OF SOCIAL MEDIA AMONG MAF PERSONNEL

Objective of Surveys:
To determine the factors influencing data leakage in the use of social media among Malaysian Armed Forces (MAF) personnel.

This survey is a part of my thesis and your coorperation is crutial for the success of the project. All responses will remain anonymous and the information will be used for educational purpose only

Please answer the questions as honestly as possible.
All responses will be treated with strictly confidential.
Thank you for participating in this questionare.

Researcher:
KAPT NUR ALFA MAZLIN BINTI MASDAN (3008509)

Section A: Respondent's Profile
The following question related to your personal data. Tick (v) at one of the options provided.

1. Please state your gender
   - □ Male
   - □ Female

2. Service Rank
   - □ Prebat/LansKoperal/Koperal
   - □ Sarjan/Staff Sarjan/Warrant Officer Class II/Warrant Officer Class I
   - □ Second Lieutenant/Lieutenant/Captain/Major

3. Work Experience
   - □ < 6 years
   - □ 6 – 10 years
   - □ 11 – 15 years
   - □ > 15 years

4. Education background
   - □ Master Degree's
   - □ Bachelor Degree's
   - □ Diploma
   - □ SPM
   - □ PMR

5. Are you aware that sharing confidential information in social media will cause of data leakage?
   - □ Yes
   - □ No
   - □ Not Sure

6. Are you frequently updating your status using social media?
   - □ Yes
   - □ No
   - □ Not Sure

Introduction

The following question in each section relate to your response towards factors influencing data leakage attributes. For all section please tick (v) the appropriate response for each item based on agreement ranging from 1 to 5.

(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)

Section B : Computer Usage Behaviour

(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)						
Question		**1**	**2**	**3**	**4**	**5**
B1	I will make sure my computer was turn off before I leaving my workstation.					
B2	I will use my friend's password to access other system that I am not authorized for.					
B3	I will always keep my email account in sign in mode to simple get the email update.					
B4	I will make sure my selecting password is strong enough using combination of symbol and alphabet.					
B5	I think about the social consequences of the confidential information that I wrote in social media.					
B6	I do not use other personal computer resources without authorization to conserve the confidential information that may exist in it.					

Section C : Security Awareness

(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)						
Question		**1**	**2**	**3**	**4**	**5**
C1	I routinely doing frequent virus update and scanning on my computer.					
C2	I allow my web browser to accept cookies from web site.					
C3	I am using an official email to send sensitive data outside the organization.					
C4	I will allow my staff using my personal computer when I am on leave.					
C5	I will write down my computer password and share with my friend.					
C6	I believe confidential information should be treated equally due to the provision of accessibility right.					

Section D : Policy Acceptance and Understanding

(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)						
Question		**1**	**2**	**3**	**4**	**5**
D1	I Know that MAF has a policy that specify they do and don't relate to ICT.					
D2	I believe the ICT policy in MAF was a comprehensive guideline for staff.					
D3	I will comply with the data security policy while performing my duties.					
D4	I fully understood by the policy and refer to the policy when facing a problem.					
D5	I believe policy acceptance and understanding is important to prevent data leakage in the use of social media.					
D6	I confused with the policy and did not understand well.					

Section E:Security Education and Knowledge

(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)						
Question		**1**	**2**	**3**	**4**	**5**
E1	I believe security education is important for all the staff that handling confidential information.					
E2	I agree that my agency needs a data security policy in ICT.					
E3	I fully understood with the policy and procedure in my organization.					
E4	I agree that educating staff through a security campaign is beneficial.					
E5	I am aware that discrimination of military information which is clarified as confidential not to share in social media.					
E6	I believe training on data security in my organization is important to all staff.					

Section F:Factors Influencing Data Leakage

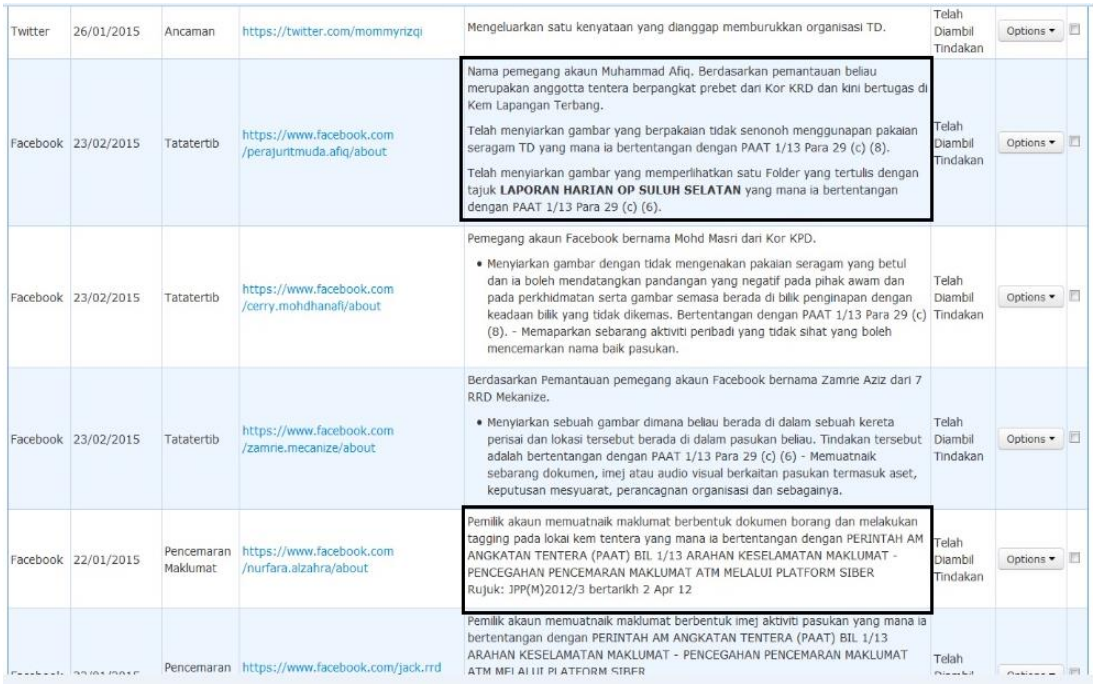
(1 – Strongly Disagree, 2 – Disagree, 3 – Nuetral, 4 – Agree, 5 – Strongly Agree)						
Question		**1**	**2**	**3**	**4**	**5**
F1	Human awareness is the first lines of defense in organization towards data leakage prevention.					
F2	Security Technology is the first lines of defense in organization towards data leakage prevention					
F3	The understanding on security policy and procedure govern in the organization will reduce the security breach and information leakage					
F4	Security training and education program should be done periodically.					
F5	The employees should given an opportunity to attend any professional certification to improve their knowledge and understanding.					
F6	Top management contribution was needed to enforce the security practice in organization					

- End of Question -

Thank You

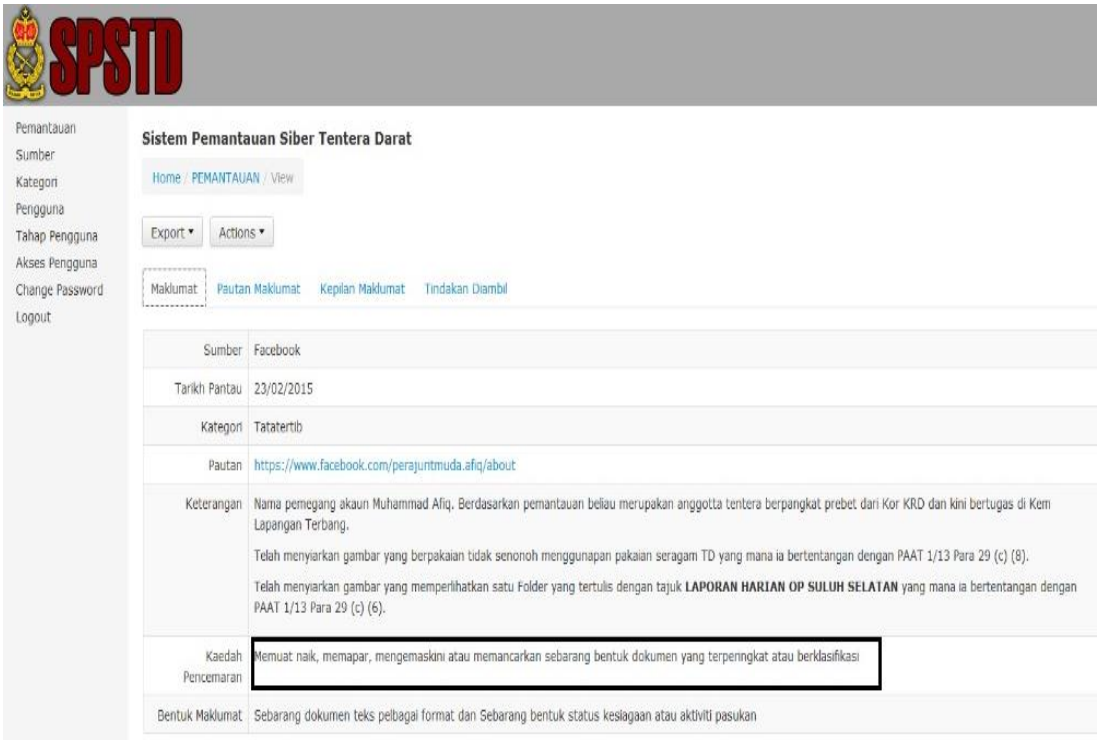
APPENDIX C

Example of case: Army Cyber Monitoring Team System – List of Monitoring



Twitter	26/01/2015	Ancaman	https://twitter.com/mommynizqi	Mengeluarkan satu kenyataan yang dianggap memburukkan organisasi TD.	Telah Diambil Tindakan	Options
Facebook	23/02/2015	Tatatertib	https://www.facebook.com/perajuntmuda.afiq/about	Nama pemegang akaun Muhammad Afiq. Berdasarkan pemantauan beliau merupakan anggotta tentera berpangkat prebet dari Kor KRD dan kini bertugas di Kem Lapangan Terbang. Telah menyiarkan gambar yang berpakaian tidak senonoh menggunapan pakaian seragam TD yang mana ia bertentangan dengan PAAT 1/13 Para 29 (c) (8). Telah menyiarkan gambar yang memperlihatkan satu Folder yang tertulis dengan tajuk **LAPORAN HARIAN OP SULUH SELATAN** yang mana ia bertentangan dengan PAAT 1/13 Para 29 (c) (6).	Telah Diambil Tindakan	Options
Facebook	23/02/2015	Tatatertib	https://www.facebook.com/cerry.mohdhanafi/about	Pemegang akaun Facebook bernama Mohd Masri dari Kor KPD. • Menyiarkan gambar dengan tidak mengenakan pakaian seragam yang betul dan ia boleh mendatangkan pandangan yang negatif pada pihak awam dan pada perkhidmatan serta gambar semasa berada di bilik penginapan dengan keadaan bilik yang tidak dikemas. Bertentangan dengan PAAT 1/13 Para 29 (c) (8). - Memaparkan sebarang aktiviti peribadi yang tidak sihat yang boleh mencemarkan nama baik pasukan.	Telah Diambil Tindakan	Options
Facebook	23/02/2015	Tatatertib	https://www.facebook.com/zamrie.mecanize/about	Berdasarkan Pemantauan pemegang akaun Facebook bernama Zamrie Aziz dari 7 RRD Mekanize. • Menyiarkan sebuah gambar dimana beliau berada di dalam sebuah kereta perisai dan lokasi tersebut berada di dalam pasukan beliau. Tindakan tersebut adalah bertentangan dengan PAAT 1/13 Para 29 (c) (6) - Memuatnaik sebarang dokumen, imej atau audio visual berkaitan pasukan termasuk aset, keputusan mesyuarat, perancagnan organisasi dan sebagainya.	Telah Diambil Tindakan	Options
Facebook	22/01/2015	Pencemaran Maklumat	https://www.facebook.com/nurfara.alzahra/about	Pemilik akaun memuatnaik maklumat berbentuk dokumen borang dan melakukan tagging pada lokai kem tentera yang mana ia bertentangan dengan PERINTAH AM ANGKATAN TENTERA (PAAT) BIL 1/13 ARAHAN KESELAMATAN MAKLUMAT - PENCEGAHAN PENCEMARAN MAKLUMAT ATM MELALUI PLATFORM SIBER Rujuk: JPP(M)2012/3 bertarikh 2 Apr 12	Telah Diambil Tindakan	Options
		Pencemaran	https://www.facebook.com/jack.rrd	Pemilik akaun memuatnaik maklumat berbentuk imej aktiviti pasukan yang mana ia bertentangan dengan PERINTAH AM ANGKATAN TENTERA (PAAT) BIL 1/13 ARAHAN KESELAMATAN MAKLUMAT - PENCEGAHAN PENCEMARAN MAKLUMAT ATM MELALUI PLATFORM SIBER	Telah	

Army Cyber Monitoring Team System - Information on selected monitoring



Army Cyber Monitoring Team System – Exhibit Attachment