Security Determinants in the Adoption of Big Data Solutions

By,

Khairulliza Binti Ahmad Salleh

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy in Information Systems

The University of Auckland

2021

Abstract

Big data has become one of the most talked about terminology across businesses and industries. The term big data is commonly described by its unique characteristics; *Volume*, *Velocity*, and *Variety (3Vs)*. At present, many organizations have adopted big data solutions (BDS) in creating competitive advantage through data-driven decision-making. However, several factors were found to hinder the adoption of BDS. Among the hindering factors are the issues of security and privacy. Various security related factors may have an impact on organizations' decision in BDS adoption, such as diverse perception on the level of complexity in securing big data environment, compatibility of organizations' current security infrastructure with the requirements of BDS, organizational information security culture, and risks in outsourcing BDS, among others. These issues in turn, created research opportunities in identifying and understanding organizational point of view in security and privacy factors that are significant in BDS adoption.

This research has explored the topic of security and privacy determinants in BDS adoption by organization through the lens of technological, organizational, and environmental (TOE) framework. This research adopted a sequential explanatory mixed-method approach that involved two-phases of data collection – a questionnaire survey followed by a case study on a single banking institution. The outcome from both phases of studies were then triangulated and this resulted in a revised conceptual framework of security determinants in BDS adoption named Sec-TOE. The framework illustrates five statistically significant factors that may positively or negatively affect organizational intention in BDS adoption, in addition to ten sub-themes of security considerations made by organizations during BDS adoption. The Sec-TOE framework provides a holistic viewpoint on security and privacy related issues in BDS adoption formed by theoretical perspective and empirical evidence.

Acknowledgements

Alhamdulillah, all praises to The Creator, the Most Beneficent and The Most Merciful, who made this journey possible by granting me patience, courage, and strength. Without His blessings, this journey would not have been possible.

I would like to thank the following people, without whom I would not have been able to complete the thesis, and without whom I would not have made it through my PhD years. First, I would like to express my sincerest gratitude to my main supervisor, Associate Professor Dr. Lech Janczewski, for his continuous support, guidance, and patience throughout these years. I will forever be indebted to you. I would also like to thank my second supervisor, Associate Professor Dr. Fernando Beltran for the motivation and guidance, particularly during my first year in the PhD program.

To my peers in ISOM department, Andrea, Ruilin, and Farzan, thank you for the stimulating discussions and friendly chats. Also, to my awesome circle of friends in Auckland, Nurulaini, Hemyza, Har Einur Azrin, and Nurul Izza, “terima kasih” for everything, especially for helping me through those “difficult” times. To my best friends, Tini and Sue, thank you for being there when I needed you the most. And to my UiTM friends; Masue, Imran, Kak Ana and Anis, I will always remember your words of encouragement – thank you.

To my support system, my family, I am forever grateful for the love, prayers, and the never-ending encouragement. Mak, Kak Aji, Yana, Abang, Aina and Aleya: I love you, and thank you for always believing in me. To my husband, Muhammad Hafizuddin, I know it has been a tough few years for you. This journey was definitely not only my own, but yours as well. Thank you for your understanding, personal support, and for being there by my side.

I would also like to thank Malaysia's Ministry of Higher Education and Universiti Teknologi MARA for the scholarship and opportunity to pursue my PhD study in New Zealand. Finally, to others who have directly/indirectly contributed to my research – I sincerely thank you!

THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Co-Authorship Form

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 5: "Technological, Organizational, and Environmental Security and Privacy Issues of Big Data: A Literature Review (2016), Procedia Computer Science Vol. 100, p. 19-28 https://doi.org/10.1016/j.procs.2016.09.119	
Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		31/5/2019

Co-Authorship Form

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 6: "Sec-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption". PACIS 2015 Proceedings. Paper 203 https://aisel.aisnet.org/pacis2015/203	
Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	85%

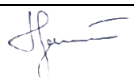
CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing
Fernando Beltran	5% editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		31/5/2019
Fernando Beltran		31/5/2019

THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Co-Authorship Form

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 7: "Adoption of Big Data Solutions: A Study on its Security Determinants using Sec-TOE Framework". CONF-IRM 2016 Proceedings. Paper 66. https://aisel.aisnet.org/confirm2016/66

Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author
Extent of contribution by PhD candidate (%)	90%

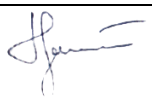
CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		31/5/2019

Co-Authorship Form

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 8: "An Implementation of Sec-TOE Framework: Identifying Security Determinants of Big Data Solutions Adoption". PACIS 2018 Proceedings. Paper 211. https://aisel.aisnet.org/pacis2018/211

Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

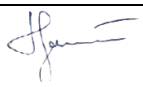
CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		31/5/2019

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

Co-Authorship Form

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 9: "Security Considerations in Big Data Solutions Adoption: Lessons from a Case Study on a Banking Institution". Procedia Computer Science, 164, 168-176. DOI: https://doi.org/10.1016/j.procs.2019.12.169

Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		29/05/2020

School of Graduate Studies
AskAuckland Central
Alfred Nathan House
The University of Auckland
Tel: +64 9 373 7599 ext 81321
Email:postgradinfo@auckland.ac.nz

Co-Authorship Form

This form is to accompany the submission of any PhD that contains published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements. Co-authored works may be included in a thesis if the candidate has written all or the majority of the text and had their contribution confirmed by all co-authors as not less than 65%.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 10: "Security Determinants in Big Data Solutions Adoption: A Mixed-method Approach" (Submitted to a journal. Awaiting for notification of acceptance).

Nature of contribution by PhD candidate	As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% editing

Certification by Co-Authors

The undersigned hereby certify that:
- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Lech Janczewski		15/06/2020

List of Original Articles (Publications)

Article 1

Ahmad Salleh, Khairulliza and Janczewski, Lech. (2016) *Technological, Organizational and Environmental Security and Privacy Issues of Big Data: A Literature Review*. Procedia Computer Science, 100, 19-28.

DOI: https://doi.org/10.1016/j.procs.2016.09.119

Abstract: This paper provides a literature review on security and privacy issues of big data. These issues are classified into three contexts; technological, organizational and environmental that is meant to facilitate future research. The main objectives of the review are to identify security and privacy issues of big data and to categorize the issues into a classification framework. The outcome of this review reveals that security and privacy issues of big data not only originate from technological deficiencies, but it may also be the outcome of organizational culture and environmental influences. At the end of review for each of the contexts, main issues were extracted and presented as potential factors that may affect organizational intention to adopt big data.

Keywords: big data, TOE framework, security and privacy, big data adoption

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.

Article 2

Ahmad Salleh, Khairulliza; Janczewski, Lech; and Beltran, Fernando (2015) *SEC-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption*. *PACIS 2015 Proceedings*. Paper 203.

https://aisel.aisnet.org/pacis2015/203

Abstract: As in any new technology adoption in organizations, big data solutions (BDS) also presents some security threat and challenges, especially due to the characteristics of big data itself - the volume, velocity and variety of data. Even though many security considerations associated to the adoption of BDS have been publicized, it remains unclear whether these publicized facts have any actual impact on the adoption of the solutions. Hence, it is the intent of this research-in-progress to examine the security determinants by focusing on the influence that various technological factors in security, organizational security view and security related environmental factors have on BDS adoption. One technology adoption framework, the TOE (technological-organizational-environmental) framework is adopted as the main conceptual research framework. This research will be conducted using a Sequential Explanatory Mixed Method approach. Quantitative method will be used for the first part of the research, specifically using an online questionnaire survey. The result of this first quantitative process will then be further explored and complemented with a case study. Results generated from both quantitative and qualitative phases will then be triangulated and a cross-study synthesis will be conducted to form the final result and discussion.

Keywords: Security and Privacy, Big Data Adoption, TOE Framework, Mixed Method Approach

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-authors.

Article 3

Ahmad Salleh, Khairulliza and Janczewski, Lech, (2016) *Adoption of Big Data Solutions: A study on its Security Determinants using Sec-TOE Framework*. *CONF-IRM 2016 Proceedings*. Paper 66.

https://aisel.aisnet.org/confirm2016/66

Abstract: Big Data Solutions (BDS) refers to innovative solutions designed to perform searching, mining and analysis of high volume of data. While BDS is being actively adopted by pioneering and leading organizations due to its prospective benefits, many organizations are still divided on the need to adopt it. Security issues related to big data's characteristics are among the hindering factors cited by non-adopters. Thus, it creates opportunities to study on the security related issues pertinent to BDS adoption. In this preliminary study, Technology-Organizational-Environmental (TOE) framework was adopted and adapted to fit the security factors being studied. Data were collected from 25 respondents through an anonymous online questionnaire and descriptive analysis was performed. The results reveal that an organization's intention to adopt BDS can be positively influenced by perceived compatibility, top management support, information security culture and organizational learning culture. Whilst, the non-adopters are negatively influenced by perceived complexity and risks in outsourcing. One factor was found to have inconclusive outcome to both adopters and non-adopters (security and privacy regulatory concern), suggesting that it may not have any significant effects in organizational intention to adopt BDS.

Keywords: Security and Privacy, Big Data Adoption, Big Data Solutions, TOE Framework, Quantitative Method

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.

Article 4

Ahmad Salleh, Khairulliza and Janczewski, Lech, (2018) *An Implementation of Sec-TOE Framework: Identifying Security Determinants of Big Data Solutions Adoption*. *PACIS 2018 Proceedings*. Paper 211.

https://aisel.aisnet.org/pacis2018/211

Abstract: Organizations are beginning to utilize big data solutions (BDS) to increase performance and creating competitive advantage. Nevertheless, some issues have been found to hinder the adoption of BDS by organizations. One of the most commonly cited issue is security and privacy. This paper presents a conceptual model named Sec-TOE with the objective of examining seven security related factors that may affect organizational intention to adopt BDS. The model is tested using SEM-PLS on a dataset of 103 organizations from New Zealand and Malaysia. The study identified five statistically significant factors; perceived complexity, top management support, information security culture, security/privacy regulatory concern and outsourcing risks. The findings of this study add to current big data and information security literature, confirms the applicability of TOE Framework in technology adoption, and contribute to organizational understanding on security related issues involved in BDS adoption.

Keywords: Big data, big data adoption, information security, TOE Framework, SEM-PLS

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.

Article 5

Ahmad Salleh, Khairulliza and Janczewski, Lech, (2019) *Security Considerations in Big Data Solutions Adoption: Lessons from a Case Study on a Banking Institution*, Procedia Computer Science, 164, 168-176.

DOI: https://doi.org/10.1016/j.procs.2019.12.169

Abstract: Adoption of Big Data Solutions (BDS) must take into consideration several issues that may affect its successful implementation, such as the issue of security and privacy. This study aims to identify security-related considerations made by organizations adopting BDS through a single case study of a Malaysian banking institution. Three main themes derived were; technological, organizational and environmental security considerations. The sub-themes identified were: challenges in securing data, capability of legacy security mechanisms, managerial security awareness, top management support, SETA, security personnel skills, employees' perception on sensitivity of information assets, regulatory compliance, reputation of BDS vendors and environmental uncertainties. The findings of this study complement current big data, information security and technology adoption research domain. It may also provide organizations with relevant information in formulating security strategies required in a big data environment.

Keywords: Big data, Big Data Solutions, Security Privacy, Case Study Banking Institutions

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.

Article 6

Ahmad Salleh, Khairulliza and Janczewski, Lech, (2020) *Security Determinants in the Adoption of Big Data Solutions: A Mixed-Method Approach.*

(Submitted for publication in a journal)

Abstract: Efficient use of big data solutions (BDS) may transform businesses by providing opportunities to mine huge volume of data and perform analytical process at a speed that was not previously possible. But, organizations seeking to adopt the solutions must first take into considerations several issues that may affect its successful implementation. One of the issues that has been acknowledged in relation to big data adoption is the issue of security and privacy. This study aims to contribute to available literature by providing empirical evidence on the technological, organizational, and environmental security and privacy factors that may affect the intention to adopt BDS, and security and privacy factors that are being considered by adopting organizations. The factors were identified by conducting a sequential explanatory mixed-method study consisting of a survey analysis on a sample of 103 organizations in New Zealand and Malaysia, and a single case study on a Malaysian banking institution. The survey identified five statistically significant security and privacy factors that may affect organizational intention to adopt BDS, while the case study produced three main themes and ten sub-themes of security-related considerations made by organizations during BDS adoption. A triangulation of results from both quantitative and qualitative data were made which resulted in a theoretical framework of security and privacy determinants of BDS adoption named Sec-TOE. The outcome of this study may contribute to academic research domain in the area of big data, information security, and technology adoption.

Keywords: Big data adoption, Big Data Solutions, Security and Privacy, Mixed-method Approach

As the first author, Khairulliza Ahmad Salleh has taken the lead in writing this article with editing done by the co-author.

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

This chapter provides an introduction of the scope of research presented in this thesis. Section 1.1 and 1.2 presents a brief discussion of the background and motivation of the research. Section 1.3 presents the research problem, formulates the research questions, and identifies the objectives of this research. The approach and paradigm for this research is introduced in Section 1.4, and a brief description of the research contribution is presented in section 1.5. Finally, section 1.6 provides an outline of the thesis structure.

1.1 Background

Over the past decade, the amount of data being generated has increased exponentially. The explosion of data is partly contributed to by the increase in development of new technologies such as location services, and social network sensors, in addition to the accelerated use of social media, and the Internet of Things phenomenon (Baig, Shuib, & Yadegaridehkordi, 2019; Lee, 2017a). The use of these new technologies essentially led to the production of massive volumes of largely unstructured and highly-variable data (Raguseo, 2018). This complex and large volume of data is often termed ‘big data’.

Even though the term big data has become ubiquitous in both academic and business circles, there is no single unified definition for the term itself in the literature (Al-sai, Abdullah, & Husin, 2019; Costa & Santos, 2017; Sheng, Amankwah-Amoah, & Wang, 2017). Hence, the term is normally described by practitioners and researchers according to its traits; including features like “volume – large amount of data”, “variety – different types of data collected”, and “velocity – speed of data transfer and creation” (Yang, Li, Elisa, Prickett, & Chao, 2019) .

Some researchers further extended the definition to include a fourth trait, "veracity – trustworthiness and uncertainties of data" (Al-sai et al., 2019).

In order to derive value from big data, technologies or solutions that can capture, store, and process large unstructured datasets are required. Amongst the solutions that are linked to big data include Hadoop, MapReduce, NoSQL, Cassandra, Hive, MongoDB, Google's Big Query, and many others (Balachandran & Prasad, 2017; Olszak & Mach-Król, 2018). Due to its predictive analytics capability, more organizations are beginning to leverage big data solutions (BDS) to create competitive advantage through data-driven decision making (Lai, Sun, & Ren, 2018; Sun, Cegielski, Jia, & Hall, 2016).

Whilst big data is expected to deliver transformative impacts to organizations, there are significant challenges associated with its use that need to be addressed by organizations (Raguseo, 2018; Rehman & Qingren, 2017; Walker & Brown, 2019). Amongst the pressing concerns in BDS adoption are the issues of security and privacy (Al-qirim, Tarhini, & Rouibah, 2017; Liu & Greene, 2020; Sun et al., 2016). Privacy and security infringements are the main risks in big data adoption and this may affect any big data initiatives contemplated in different industries (Rehman & Qingren, 2017; Shahbaz, Zhai, Shahzad, Hu, & Gao, 2019).

Big data security issues may be further aggravated by the wide area deployment of big data infrastructure and the inability of traditional security solutions to scale up to big data's security requirements (Kourid, Chikhi, & Hong, 2017; Moura & Serrao, 2016; Soliman, 2019). Some big data initiatives undertaken by organizations have failed due to "unclear security controls" (Prakash, Prithiviraj, & Mary, 2018), reinforcing the point that security is one of the most important aspects to consider during big data adoption (Park & Kim, 2019). Furthermore,

security and privacy issues have often been cited as one of the most important factors hindering the further adoption of BDS (Nguyen & Petersen, 2017; Watson, 2019). It is therefore important and significant for organizations to be aware of these issues in order to ensure that their big data investments reap their intended benefits.

While security and privacy challenges in big data environment have been highlighted in various reports and publications (Chenthara, Wang, & Ahmed, 2018; Latif et al., 2019; Thales & 451 Research, 2018; Zaki, Uddin, Hasan, & Islam, 2017), there is a paucity of empirical research on security factors that may (or may not) affect the intention of organizations to adopt BDS within the information systems research community (Raguseo, 2018). Hence, it is important for issues of security and privacy to receive as much attention as other BDS adoption criteria since they play an important role in influencing organizational intentions towards BDS adoption.

1.2 Motivation

Security threats and challenges are pertinent issues that need to be addressed during the stages of new technology adoption in organizations. This point is equally relevant when considering the adoption of BDS (Samet, Aydin, & Toy, 2019). When viewing big data solutions from a security perspective, two separate domains can be considered. The first domain looks at security challenges and risks associated with a big data environment (Chenthara et al., 2018), whereas, the second domain revolves around the use of big data technologies and solutions for security intelligence (e.g. use of big data analytics to identify anomalies, threats, alert verification, fraud detection, etc.) (Shatnawi, Yassein, Abuein, & Nsuir, 2019). Prior studies have found that security issues and challenges are amongst the key factors hindering the

adoption of BDS (Nguyen & Petersen, 2017; Watson, 2019), hence, the main interest of this research is to study firstly the security-related domain. This research will focus on organizational security issues in BDS adoption instead of looking at the application/adoption of BDS as a security mechanism.

Details of security threats and challenges encountered in organizational BDS environments have appeared in numerous reports and articles (Duncan, Whittington, & Chang, 2018; IDC, 2019; Latif et al., 2019). Within academic settings, most of the arguments about these threats and challenges are not based on empirical studies, but instead, were written based on article reviews and simple surveys and are therefore anecdotal in nature. While several studies do provide empirical findings on security issues involving big data, they are primarily focused on technicalities such as securing big data platforms, its infrastructure and software framework, as well as algorithm development (e.g. Jain, Gyanchandani, & Khare, 2019; Johri, Arora, & Kumar, 2018; Kourid et al., 2017; Yang et al., 2019).

Although these findings and reviews are beneficial for both practitioners and academics, there remains a scarcity of empirically based findings looking specifically into security and privacy factors that may affect organizational intentions to adopt BDS. In addition, although many security considerations involved in the adoption of BDS are in the public domain, it remains unclear whether these commonly held perceptions and publicized facts have any actual impact on the adoption of the solutions. Hence, this became the main motivation for the research, where the multi-paper thesis is expected to provide further empirical contributions to the existing literature on big data adoption in general and more specifically on the security determinants of BDS adoption.

As many organizations are already using BDS in their operations, either in specific departments or as supporting solutions to their enterprise wide information systems, it will be beneficial to study the security factors that are of concern to them and identify the role that these security concerns play in the decision to adopt solutions. Security experts have also noted that during the process of new technology adoption, organizations tend to view security issues only as an afterthought (Bastos, Shackleton, & El-Moussa, 2018; Herath, Herath, & D'Arcy, 2020). In fact, there is a tendency to consider it in isolation (Loukaka & Rahman, 2017). Thus, in the case of BDS adoption, organizations are vulnerable to security threats and considerable pushback when they fail to properly consider the impact of security related issues (Nguyen & Petersen, 2017; Rehman & Qingren, 2017; Torre, Dumay, & Rea, 2018).

If the security factors related to BDS are overlooked, amongst the potential consequences include the loss of confidentiality, integrity and availability of data (Watson, 2019). This in turn, may lead to reputational harm and legal repercussions for an organization (Chen et al., 2016; Watson, 2019) . With big data, it should be a priority for organizations to ensure that security aspects receive continuous attention during the whole process of adoption and assimilation (Samet et al., 2019). This aspect also motivates this research to look at security as a prime consideration before the adoption of new technology instead of focusing on security at a later stage of adoption.

Information Systems (IS) is a field of research that draws on theories from multiple areas. Within this field, the areas of technology adoption, acceptance, diffusion and use, may be considered as one the most established streams of research. Numerous theoretical perspectives and technology adoption models have been introduced and used as a guide when conducting research in innovation/technology adoption. Information security, however, is one of the

research streams in IS that has less empirical research within the technology acceptance, adoption, diffusion and use literature (Salahshour et al., 2018). At present, the practice of securing information systems and assets in organizations is growing in complexity thus gaining added importance. This is due to the growing number of security and privacy related incidents, financial repercussions resulting from unauthorized access to information, and negative publicity arising from information security breaches. A study by Gartner (2016) found that more than three-quarters of organizations surveyed are investing or have the intention to invest in big data. Therefore, a detailed understanding of the security and privacy related factors that influence organizational adoption of BDS is both critical and timely. In spite of this, reviews carried out on hundreds of journal articles and conference proceedings regarding big data, revealed that the amount of research that studied the factors influencing adoption is still relatively small (Chen et al., 2016; Salleh & Janczewski, 2016). These findings were one of the prime motivations for the researcher to focus on information security factors related to BDS adoption.

1.3 Research Problem and Research Objectives

Accordingly, based on the issues and points of motivation identified earlier, the following research problem is formulated:

There is a need for organizations that have the intention to adopt BDS to be aware of the security related factors that may positively or negatively affect the intention to adopt. This awareness is needed to strengthen organizational security preparation during the whole process of BDS adoption and assimilation.

In order to address the above research problem, the researcher adopted a two-phase, sequential explanatory mixed-method study to examine the security factors or determinants influencing BDS adoption. This research focuses on the influence that various security technological factors, organizational security factors, and security related environmental factors have on BDS adoption. Hence, the main objective of this research is as follows:

To provide a conceptual security based BDS adoption framework as a guide for organizations planning to embark on big data initiatives.

To achieve the main objective identified above, the following two ancillary objectives were identified for the research:

1) *To examine security determinants by focusing on the influence that various security technologies, organizational security view, and security related environmental factors have on BDS adoption.*

2) *To ascertain the security and privacy-related considerations made by organizations in the process of BDS adoption.*

The objectives stated above focused on various gaps in current knowledge, which are then addressed in this research by formulating the following research questions:

1) *What are the main themes related to big data's security and privacy issues?*

2) *How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption amongst adopter and non-adopter organizations?*

3) *How do technology factors in security, organizational security view and security-related environmental factors encourage/discourage organizations' big data solution adoption?*

4) *Do organizations consider security-related factors during BDS adoption and if so, what considerations are made?*

5) *What recommendations on security-related determinants can be introduced for organizations adopting big data solutions?*

Table 1-1 shows the research problem, objectives, and research questions addressed in this thesis. Each research question was then addressed separately in different original articles forming a part of this thesis.

Table 1-1: Research Problem, Research Objective, Research Questions and Its Associated Article Number and Chapter

Research Problem	There is a need for organizations that have the intention to adopt BDS to be aware of the security related factors that may positively or negatively affect the intention to adopt. This awareness is needed to strengthen organizational security preparation during the whole process of BDS adoption and assimilation.	**Article number**	**Chapter**
Main Research Objective	To provide a conceptual security based BDS adoption framework as a guide for organizations planning to embark on big data initiatives		
Research Question 1	What are the main themes related to big data's security and privacy issues?	Article 1	5
Research Question 2	How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption amongst adopter and non-adopter organizations?	Article 3	7
Research Question 3	How do technology factors in security, organizational security view, and security-related environmental factors encourage/discourage organizations' big data solution adoption?	Article 4	8
Research Question 4	Do organizations consider security-related factors during BDS adoption and if so, what considerations are made?	Article 5	9
Research Question 5	What recommendations on security-related determinants can be introduced for organizations adopting big data solutions?	Article 6	10

Chapter 4 will provide further discussion on the research questions, main objectives of the research, and the research process. In the next section, the paradigm and approach of the research are briefly explained.

1.4 Research Approach and Paradigm

This section briefly explains the research approach and design of this multi-paper thesis. The main research approach adopted is sequential explanatory mixed-method approach (Creswell & Clark, 2018), which basically consists of two methods of data collection – quantitative and qualitative. First, the philosophical perspective of the research is presented, followed by a brief description of the methods used in data collection and data analysis.

Research is normally based on some underlying philosophical assumptions or paradigm that acts as "a guide that a researcher can use to ground their research" (Shannon-Baker, 2016). The three main paradigms are; positivist, interpretive and critical. The implementation of these paradigms in research follows a set of distinctive methodological strategies (De Villiers, 2012). However, due to the mixed-method approach of this research, it does not belong to a single philosophical paradigm. While the quantitative phase of the research is closely linked to *positivist* stance, and the qualitative phase to *interpretive*, these two methods when combined into a single research, did not lend itself into any of the three paradigms described earlier, as both methods/phases have different underlying assumptions.

Thus, the research is best associated with *pragmatism* – a paradigm that is typically linked to mixed method research (Teddlie & Tashakkori, 2009). *Pragmatism* as a paradigm mainly focuses on the problems that need to be researched and its consequences (Creswell & Clark, 2018; Feilzer, 2010), and "the use of multiple methods of data collection to inform the problems under study" (Creswell & Clark, 2018). Hence, by associating this research with *pragmatism*, the guiding principle is to identify "what works" in answering the research problem and real-world practice.

This research looks at security determinants that may affect BDS adoption in organizations. For this research, two main data collection techniques were used (sequential explanatory mixed method). The first quantitative phase used a survey to test a conceptual framework of BDS adoption. Once the first phase was completed, the second phase proceeded with a single case study. This qualitative phase employed semi-structured interviews with pre-formulated questions and document observation as the primary and secondary data collection technique. Results of the second phase of research (the case study) provided validation for the results of the first phase quantitative survey. A detailed explanation of the research approach can be found in Chapter 4 as well as in each article reporting the process and outcome of each stage of the research.

1.5 Research Contributions

The findings of this research have several contributions towards the research domain as well as some practical implications. Amongst the contributions of this research are; it is one of the earliest empirical studies on technological, organizational, and environmental (TOE) security-related determinants in BDS adoption. The research also introduced security determinants in BDS adoption framework (Sec-TOE) that may assist organizations in identifying factors that may facilitate or hinder adoption. In addition, the research presented in this thesis also led to several publications – two in Association for Information Systems (AIS) conferences and three in AIS affiliated conferences.

As for practical implications, the Sec-TOE framework introduced may benefit managers, security professionals and IT service providers/vendors by presenting the specific security and privacy related issues that may affect organizational intention to adopt BDS. Other

contributions and practical implications of this research will be discussed further in the final chapter (Chapter 11).

1.6 Thesis Structure

Included in this thesis are multiple original articles that present the outcome of different stages of the research. The following Figure 1-1 is a visual depiction of the final thesis structure.

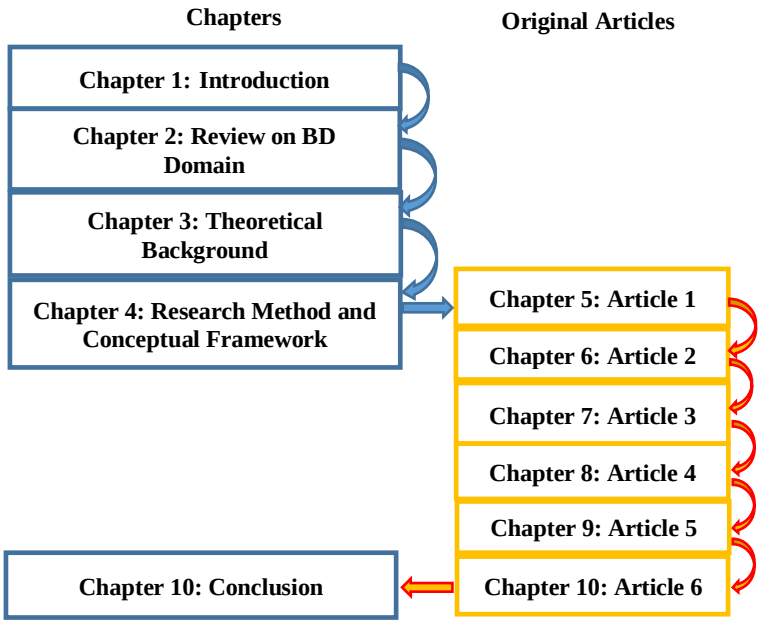


Figure 1-1: Structure of the Thesis

The detailed framework of the whole research process and the relationship of the research questions to the published original articles are presented in sub-chapters 4.2 and 4.6 respectively.

2. REVIEW OF ISSUES IN BIG DATA DOMAIN

The objective of this chapter is to present a review of relevant literature in relation to issues and concepts in the big data domain. Each original article included in this thesis has its own literature review section, thus this chapter aims to provide a starting point for the basic concept of big data, Big Data Solutions (BDS), big data adoption, general security, and privacy issues in big data. It differs from Article 1, where a literature review process was carried out to identify specific security and privacy issues in big data. The identified issues were then classified into a classification framework and used in the theoretical framework introduced in Article 2. This chapter begins by defining the concept of big data, followed by BDS, and BDS adoption.

2.1 Definition of Big Data and Big Data Solution (BDS)

Various definitions of big data were found during the process of literature search and review in preparation for this research. These various definitions indicated that there is not a universally accepted definition for the term big data. Even though the term is now being presented as amongst the "buzz-words" in this current era, consistent definition for this emerging and expanding phenomena is still lacking (Al-sai et al., 2019; Baig et al., 2019; Frizzo-Barker, Chow-White, Mozafari, & Ha, 2016).

The following section will discuss the various definitions of big data in general before arriving at a single definition that will be adopted in this research.

2.1.1 Defining Big Data

The initial description of big data and its characteristics was said to have emerged from a report written by Douglas Laney, a Gartner Inc.'s analyst back in 2001. In the report, Laney described the challenges and opportunities in data growth by the use of three factors: volume, velocity and variety of data (Laney, 2001). The term volume refers to the size of data set, velocity describes the speed of data being created, and variety refers to the various data sources and types (Baig et al., 2019; Yang et al., 2019). This 3Vs definition has since found its way to various industrial reports, technology magazines as well as academic articles. In 2012, Gartner updated their initial definition of big data. Retaining the 3Vs characteristics of data, they defined big data as "A high-volume, high-velocity and/or high -variety information asset that requires new forms of processing to enable enhanced decision making, insight discovery and process optimization"(Gartner Inc, 2012). Mayer-Schoneberger and Cukier (2013) gave a broader definition when they related big data to the novel ways for society to generate beneficial insights, and, to produce noteworthy goods and services.

Even though most definitions of big data have included the 3Vs in describing its characteristics, some scholars and industry players have extended the Vs to a fourth V (Al-sai et al., 2019; Sun et al., 2016) and some even to 5Vs (Bertino & Ferrari, 2018; Kourid et al., 2017; Terzi, Terzi, & Sagiroglu, 2016). These extra Vs were added to the initial 3Vs according to the requirements of a particular research or as further explanation to the existing definition of big data (Chen & Zhang, 2014). Value and veracity are most often quoted as the fourth and fifth characteristics of big data. The added value that can be derived from the collected data, its predictive ability, and usefulness in supporting the decision making process is what the fourth V (value) refers to (Chenthara et al., 2018; Sheng et al., 2017). As for veracity, it refers to uncertainty of data; its consistency and trustworthiness (Abbasi, Sarker, & Chiang, 2016;

Yang et al., 2019). One paper was identified in the literature which steered away from using another "V" by describing *complexity* as the fifth characteristic. According to the authors, complexity "measures the degree of interconnectedness (possibly very large) and interdependence in big data structures" (Kaisler, Armour, Espinosa, & Money, 2013).

Following on from the above discussions, one general observation on big data can be made; big data consist of huge data sets, with various data types and sources, produced and transferred at great speed, thus creating some difficulty in managing and processing it using traditional data processing techniques and saving it in any traditional structured relational database management systems. The data types can be structured, semi-structured and unstructured, collected from web and social media (e.g. clickstream data which are information on the sequence of pages or path taken by users as they navigate a website), and require processing by data processor or data analyst (Mohamad, Selamat, & Salleh, 2019; Watson, 2019).

For this research, the definition of big data as proposed by Gartner was adopted. Thus, big data is defined as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (Gartner Inc, 2012). This definition is well suited for the purpose of this research as it incorporates the essence and characteristics of big data.

In the next section, a discussion of the term big data solution (BDS) will be offered. This is necessary to distinguish between the concept of big data itself with the technologies and tools that are used in support of big data.

2.1.2 Defining Big Data Solution – Technologies and Tools Supporting Big Data

To make big data manageable and useful for analytical purposes, organizations need to investigate new supporting technology. As discussed in the previous section, big data is normally associated with large volume, high velocity, and variety of data. Thus, to fully harness the potential of big data, organizations will have to search for technologies that have the ability to process and analyze various sources of data, such as data in textual format, social media, clickstreams, or analyze data streams from Internet of Things (IoT) (Arfat, Usman, Mehmood, & Katib, 2020; Watson, 2019). Due to the changes and advances in technology solutions that are closely related to big data, a transformation in the manner of storing and processing of data, as well as the hardware and software is required (Arfat et al., 2020). These technologies are now available for selection and deployment by organizations.

Discussions on the technologies and solutions for big data are abundant. Most of the discussions on technology supporting big data often focused their attention on what is new with these technologies. The focus is often directed to the way these technologies are able to cater to large volumes and unstructured format of data (Sheng et al., 2017). With the changing nature of data (multiple formats of data - unstructured and streamed) being captured by organizations, these new technologies are expected to be able to process and provide storage for types of data that cannot be handled through the use of solo servers and traditional relational database management system (Prakash et al., 2018). It is well known that traditional relational databases treat data in rows and columns, which is not feasible to handle big data that varies in terms of format. Hence, due to the inability of these traditional databases to store big data, organizations have started to deploy new solutions specifically tailored for big data. In relation to this, software vendors have now come up with a new generation of data processing software and applications (Arfat et al., 2020). Hadoop, or more often referred to as Apache Hadoop, is one

such software tool. Hadoop is regularly mentioned in reports and articles that discusses about the technologies and solution used in big data and analytics (Costa & Santos, 2017; Johri et al., 2018; Johri, Kumar, Das, & Arora, 2017; Shatnawi et al., 2019). It is popular for being the framework that can divide data across multiple computers, offers unified storage, and is highly scalable to big data's high data volume. The most common version of Hadoop is the open-source Apache Hadoop, while at present; many commercial vendors have also created their own version of Hadoop, such as the Cloudera, Hortonworks, MapReduce, and Amazon. These commercial Hadoop are normally added with enterprise support and added functionalities (Kataria & Mittal, 2014; Watson, 2019). MapReduce is one other software tool that is regularly associated with processing and producing large data sets (Balachandran & Prasad, 2017). Originally a proprietary Google technology (now genericized), MapReduce is a software framework that allows division of big data for processing across large clusters (Arfat et al., 2020).

There has been a dramatic change in the technology environment for big data over the past few years and it will continue to change soon. Present changes can be seen in the birth of new forms of databases that can handle unstructured data, with most being NoSQL compliant (NoSQL is often defined as "Not only SQL" or "Not Relational")(Costa & Santos, 2017). Several new scripting languages that are interactive in nature, i.e. Pig, Hive and Python have also emerged. Davenport (2014) points out that another main aspect of the big data technology environment that differs from traditional information management is in the handling of volume and velocity of data, which can swiftly alter segregation methods typically found in traditional data analysis.

The above nature of big data has opened the market for software vendors to design and produce software that is able to provide support for organizations interested in leveraging big data and

its analytical power. The technologies mentioned above will form an ecosystem that is used to perform processing of big data or more commonly referred to as big data analytics (Balachandran & Prasad, 2017; Lai et al., 2018). The use of big data analytics can have different modes depending on the objective of its use and are essentially being applied by organizations in different industries with different expectations and perceived outcomes (Shatnawi et al., 2019).

Based on the brief discussion above on the software, framework, and scripting language associated with big data analytics, it can be established that big data solutions (BDS) will consist of various collection of functions. These technologies are able to provide high-performance analytical support and processing of large data sets typical in big data environment (Lee, 2017b). Hence, in relation to this research, BDS is defined as a collection of technologies and frameworks that provides a "platform to integrate, manage, and apply sophisticated computational processing to large datasets" (Davenport, 2014). These solutions can be utilised by organizations to create value from data that they own and produce actionable information and knowledge that may improve services and operations across organizations.

2.2 Big Data Adoption and Big Data Adoption Research

Big data is now relevant across industries and economic sectors (Baig et al., 2019; Bremser, 2018). This is in part due to the proliferation of digital data, and the amount of data being produced across industries and in data-intensive organizations. Looking at the benefits of big data application specifically in terms of its ability to store, accumulate and combine large datasets, organizations are now aware of how big data will enable rigorous data processing, thus making deep analyses of data more accessible (Barbosa, Vicente, Ladeira, & de Oliveira,

2018). Pioneering business and organizations have started to exploit the benefits of big data in creating value for their operations in order to remain competitive (Olszak & Mach-Król, 2018). Not only in businesses, the use of BDS can also be found in the government sector, providing a boost to public sectors' productivity and offered services (Klievink, Romijn, Cunningham, & de Bruijn, 2017). Due to this increasing awareness of the applicability and advantages of BDS in multiple settings and functions, numerous studies have been conducted in relation to big data platform and technologies, security concerns and privacy impact of big data, as well as studies on the suitability of utilizing BDS in specific sectors and industries. Much of these scholarly research in big data focuses on technical algorithm and system functions (e.g. Johri et al., 2018; Mohamad et al., 2019; Samuel, Sarfraz, Haseeb, Basalamah, & Ghafoor, 2015; Soliman, 2019).

There are also quite a number of big data survey reports that came from technology provider companies and market research organizations (e.g. Dresner Advisory Services, 2017; IDC, 2015; NewVantage Partners, 2019; Sapio Research, 2019). In a report by New Vantage Partners (2019), the findings of a survey conducted on big data and artificial intelligence adoption shows that there is greater urgency to invest in big data initiatives - with 87% of the respondents confirming this urgency.

Thus, it is crucial and timely to understand the internal and external factors that may have an impact on organization's big data adoption endeavours. This is especially beneficial as the quantum of research on BDS adoption within organizations is still scarce (Cabrera-Sanchez & Villarejo-Ramos, 2019; Verma, Bhattacharyya, & Kumar, 2018). The following section provides an overview of big data adoption in organizations as well as a brief look at the research done in the big data domain.

2.2.1 Big Data Adoption and Application in Various Sectors and Industries

Data is now being collected and produced at an unprecedented scale. This trend is evident in various industries that have traditionally worked with vast amounts of data, for instance, the telecommunication and finance industries (Dresner Advisory Services, 2017). Presently, other industries are also aware of big data's potential. This is where BDS enters the picture and it has since seen its application in broad and diverse range of areas. BDS is now deployed to support analytic processes in numerous industries such as retail, manufacturing, and health to name a few (Abbasi et al., 2016; Al-sai et al., 2019).

Amongst the earliest organizations and businesses that have embarked on big data analytics projects are the British retail giant Tesco Plc, and Capital One, a financial institution. Even though Tesco is a brick-and-mortar supermarket chain, it managed to collect transaction data from its millions of customers through its loyalty card scheme called *Clubcard* (Patil, 2014). From this loyalty program, Tesco can analyse new business prospects, such as targeting promotions to specific customer segments as well as helping them in making decisions on pricing, and even shelf allocation. Seeing the success of their big data analytics venture, Tesco even began to apply it in optimizing its stock keeping system by using historical sales and weather data to forecast sales (P. Liu & Yi, 2018; Mishra, Gunasekaran, Papadopoulos, & Childe, 2018; Patil, 2014).

Whereas for Capital One (one of the earliest financial institutions that adopted BDS), big data is being capitalised upon for segmenting their credit card customers. The outcome of this process is the ability of Capital One to offer tailored products according to the individual risk profiles of their customers (Mazzei & Noble, 2017). Social media is another medium where data can be collected by organizations to measure the immediate impact of their marketing

campaigns and brand perception. Ford Motor and PepsiCo are two examples of organizations that use big data analytics to analyse consumer postings made about these two organizations on popular social networking sites such as Facebook and microblogging site Twitter (Hofmann, 2017; Sivarajah, Irani, Gupta, & Mahroof, 2020).

Another example of an industry that has started to utilize BDS is the healthcare industry. In an article that queried the readiness of urologist in harnessing big data for health care and research, Ghani *et al.* (2014) noted several instances where big data was being applied in the healthcare industry. Amongst those listed are the use of big data approaches in genomics and health-related social media (Ghani, Zheng, Wei, & Friedman, 2014). Further, The American Society of Clinical Oncology has developed a platform called CancerLinQ, which combined information from electronic health records and genomic data, with the aim of delivering cancer patients targeted measures in cancer therapy (Mayo et al., 2017; Rubinstein & Warner, 2018).

BDS is not only seen as beneficial by business organizations, it has also garnered the interest of several federal governments. The United States for instance, announced a "Big data Research and Development initiative" back in 2012 with an estimated funding of $200 million dollars. The initiative is spearheaded by six federal agencies; the National Science Foundation, National Institutes of Health, Department of Defence, Department of Energy and United States Geological Survey (Alley-young, 2017). Collectively, these six federal departments and agencies are expected to improve the tools and techniques as well as methods to extract, organize and gather insights from large and complex data sets (Chakravarthi & Srinivas, 2017). In addition, a Southeast Asian country - Malaysia, also announced a national big data initiative at the end of 2013. Malaysia's big data initiative is led by the Communications and Multimedia Ministry with the support of the Malaysian Administrative Modernisation and Management

Planning Unit (MAMPU), and Multimedia Development Corporation (MDeC) (Abdullah, Ibrahim, & Zulkifli, 2017). They jointly initiated and implemented four big data analytics pilot projects within four government agencies. The four pilot projects were; a price watch project, sentiment analysis, crime prevention, and infectious disease forecasting (Dzazali, 2014). Lessons learnt from the pilot projects lead to the development of Big Data Analytics Implementation Guidelines for Public Sector in 2016 (Dollah & Aris, 2018).

While the above examples demonstrate successful implementation and launched initiatives of big data analytics, some organizations are still hesitant to embark on big data projects. In the report of a survey done by Dataguise (2016), 73% of the surveyed enterprises revealed that their big data initiatives were either delayed or terminated in response to data security concerns. These findings indicate that security issues and concerns may have a direct impact towards organizational intentions to adopt BDS.

As illustrated in the above discussion on the adoption and application of big data in various industries and sectors, it is safe to conclude that BDS is gaining momentum in its acceptance and importance across industries. Nonetheless, there are still issues and challenges in relation to big data, which dampens prospects for adoption by businesses and organizations (Cabrera-Sanchez & Villarejo-Ramos, 2019; Raguseo, 2018). These issues in turn have created research opportunities to comprehend the factors pertinent to big data adoption in organizations (Olszak & Mach-Król, 2018). Hence, it became one of the motivating factors for this research to explore the issues hindering adoption, specifically from security aspects (being frequently cited in the literature as one of the main reasons hindering the adoption of big data), that may encourage or discourage the adoption of BDS.

The following subsection will briefly overview the research publications within the big data domain to demonstrate the scarcity of academic literature studying big data adoption factors in organizations.

2.2.2 Overview of Big Data Adoption Research

While the adoption of BDS is rising, till date, the number of studies that have made empirical findings on the adoption of BDS in organizations is still limited (Baig et al., 2019; Nguyen & Petersen, 2017; Verma et al., 2018). The following Table 2-1 shows some of the recent studies carried out in relation to BDS adoption.

Although the list of studies conducted in BDS adoption shown in Table 2-1 is not exhaustive, it can be summarized that the focus of these studies was on general factors that may facilitate BDS adoption and its various challenges. Besides the studies done in the academic domain, there were also studies and surveys on BDS adoption conducted by market research companies and consulting/technology firms, e.g. (Dresner Advisory Services, 2017; NewVantage Partners, 2019; Sapio Research, 2019).

In addition, there are also articles that looked into the suitability, influences, and current application of BDS in certain industry and specific business function, e.g. articles by (Al-Rahmi et al., 2019; Li, Wu, Liu, & Li, 2015; Yadegaridehkordi et al., 2018). The above overview of current work on BDS adoption in organizations illustrates that empirical work on identifying the factors that have significant impact on organizations' BDS adoption is still in its infancy. It is thus beneficial to explore the evidence gathered by non-scholarly outlets and expand it further in academic research. This research aims to further identify organizational

conditions and variables that may encourage or discourage organizations' big data adoption strategies.

Table 2-1: Studies on Big Data Adoption

Topic	Research Approach	Authors
Highlight different components, theoretical implications, and drivers and challenges of BD adoption.	Literature Review	Al- Qirim, Tarhini and Rouhibah (2017); Baig, Shuib, and Yadegaridehkordi (2019)
Factors affecting big data analytics adoption in companies.	Content Analysis Survey Case Study	Sun, Cegielski, Jia and Hall (2016); Agrawal (2017); Cabrera-Sánchez and Villarejo-Ramos (2019); Walker and Brown (2019); Park and Kim (2019)
Investigation on the adoption levels of BD technologies in companies, benefits, and risks related to the usage of BD technologies by companies.	Survey	Raguseo (2018)
Assessment on organizational readiness in BD adoption.	Literature Review and Interview	Olszak and Mach-Król (2018)
Addressing the factors determining firms' intention to adopt BDA. Classify potential factors into four categories.	Survey	Lai, Sun and Ren (2018)
Interdepencies of contextual factors in BD adoption.	Survey	Schull and Maslan (2018)
Analysis on current approaches for the exploration of new BD potentials (initiation phase), and factors that influence the choice of approach.	Case Study	Bremser (2018)

Another stream of research in the big data domain is security and privacy. Security and privacy issues have consistently appeared in the literature as factors that pose challenges in the adoption of BDS (Venkatraman & Venkatraman, 2019; Watson, 2019) . Security factors have also been

cited as one of the hindrances in the adoption of BDS by organizations (IDC, 2019). However, most of the existing academic literature only provides an overview of the potential challenges with respect to security and privacy in a big data environment. Among the articles are an article by Chentara, Wang and Ahmed (2018) that listed a set of challenges, scope, as well as techniques used to secure privacy, and security for big data, and an article by Gupta and Ruhil (2020) that presented an analysis on the technical challenges of implementing big data security and privacy protection, as well as offering key solutions to address the issues. Other research in security and privacy of big data were more inclined towards developing algorithms and introducing new mechanisms in ensuring data security and privacy in a big data environment (Jain et al., 2019; Johri et al., 2018; Soliman, 2019).

Although security and privacy concerns of BDS has been highlighted in numerous literatures, to date, however, there has been little discussion about the actual security factors that may hinder the adoption of big data by organizations (Nguyen & Petersen, 2017). In addition, besides the results from non-scholarly studies conducted by marketing research firms, no research has been found that specifically surveyed organizational concerns on the security factors that are associated with BDS. In relation to this, Raguseo (2018) stated the need for organizations to be aware and consider security and privacy issues before investing in BDS, as these issues are the two most recognized risks cited by organizations that participated in the study. As a result of the above concerns, it is the intention of this research to study the security and privacy related conditions and variables that may impact an organization's intention in adopting BDS. The following section will provide a discussion on information security concerns and practices in organizations, and the subsequent section will provide an overview of security and privacy concerns in relation to BDS.

2.3 Information Security Concerns and Practices in Organizations

According to the 2019 Thales Data Threat Report produced by IDC, 60% of their global respondents have experienced data breach, and the number is even higher in the US, with 65% of the respondents surveyed having experienced security breaches. Respondents of the survey also acknowledged that their organization are vulnerable - with 86% of them stating that they are vulnerable to data security threats. Globally, 34% categorized themselves as "very" or "extremely" vulnerable (IDC, 2019). Hence, organizations realizing the extent and severity of security breaches and incidents should place high importance on the management of risk and security (Raguseo, 2018). Fundamentally, security risk management and assessment should also be an important driver in any new technology adoption process in organizations.

The following section will provide a brief discussion on the security and privacy concerns specifically in relation to BDS. Big data solutions, seen as new technology innovation, have its own set of characteristics that could potentially lead to specific security and privacy issues.

2.3.1 Security and Privacy Concern for Big Data Solution

Security and privacy factors have consistently appeared as one of the challenges in BDS application and implementation (Singh, Halgamuge, Ekici, & Jayasekara, 2018; Venkatraman & Venkatraman, 2019). In handling big data, organizations must be prepared to protect data that is expanding in volume, variety, and velocity. These main characteristics of big data, the 3Vs, warrants a more solid data governance strategy (Su, 2019). In addition, for any big data environments, data will be transferred and moved in between structured, unstructured, and semi-structured formats while it flows through various applications and analytical processes. This feature will be against the traditional concept of data silos where data security governance

is normally applied separately within each silo (Watson, 2019). Security governance that focuses on data silos may no longer be sufficient as it will lead to incoherent data security policies and management, thus enhancing the probability of inducing security turmoil (Yang et al., 2019). Next, discussion on security and privacy concerns in BDS will continue within the following three headings: technological security concern, organizational security concern, and security and privacy related environmental concern.

Technological Security Concern

The characteristics that are often associated with big data; the volume, variety and velocity may contribute to security issues for organizations (Jain et al., 2019; Prakash et al., 2018). Each of these characteristics will pose certain security concerns that require a strong security solution and technologies in ensuring the confidentiality, integrity and availability of data (Kourid et al., 2017). For organizations that failed to recognize and separate big data and traditional non-big data, it may lead to a failure in deploying a proper security technology and solution in protecting their big data. Moura and Serrao (2016) point out that existing non-big data security solutions that are tailored to "private computing infrastructures, confined to a well-defined security perimeter, such as firewalls and demilitarized zones (DMZs) are no more effective".

Thus, it is important for organizations seeking to embark on big data initiatives to recognize the unique characteristics of big data that undoubtedly will lead to new security and privacy threats (Ashabi, Sahibuddin, & Haghighi, 2020). A fit between an organization's current security technology and the intended big data solution adoption and implementation should be amongst the factors to consider when making decisions to adopt big data solution.

The first characteristic of big data - *Volume*, which refers to the huge size of data set collected and created from a diverse range of sources, may contribute to security issues due to the sheer amount of data involved (Jain et al., 2019). High data volume would present a danger in security, for example, it may attract the attention of cybercriminals and could lead to security breach (Torre et al., 2018). Security incidents involving organizational IT systems and data theft are prevalent at present, and with the availability of large and huge amounts of data typical in a big data environment, it represents an alluring target for cybercriminals (IDC, 2019). In essence, this characteristic of big data poses a challenge to existing security technologies and solutions. One of the key challenges is to provide security technologies and solutions that are able to scale to the large size of data sets and distributed nature of big data (Gupta & Rohil, 2020).

The second general characteristic of big data, *Velocity*, which describes the speed in which data are being created and the speed at which it should be analysed and acted upon, may also pose some security threats (Terzi et al., 2016). Many organizations are currently generating high frequency of data and this may create difficulties in maintaining the security of data. Among the security issues that may be associated with the rapid frequency of data creation is the lack of technological security capabilities to have secure storage for large amounts of data particularly during peak data traffic (Soliman, 2019; Venkatraman & Venkatraman, 2019). In addition, rapid data flows will increase the need to have a security technology with the ability to screen and audit access while at the same time protecting data stored across silos.

As with the other two general characteristics of big data, the third characteristic, *Variety*, also poses significant security issues and challenges (Terzi et al., 2016). Variety refers to the various data sources and types of data being collected and stored in any big data environment. Data

collected can be in the form of structured, semi-structured and unstructured data. Thus far, organizations are familiar in the handling of the security measures in protecting structured data, but with the combination of unstructured data, the experience in ensuring security may be lacking (Venkatraman & Venkatraman, 2019). When data are collected from a variety of sources, one key security issue that may arise is the issue of input validation and untrusted input sources (Mishra & Singh, 2017). It will be difficult to identify malicious data sources, and the need to filter malicious input from the diverse range of data sources will also be a daunting process.

The above discussion has specified some of the security concerns that require appropriate technology solutions to ensure security of data collection and storage in a big data environment. Organizations need to be fully aware of the security concerns and issues associated with big data, especially those that are contributed by its general characteristics, the volume, velocity, and variety. By acknowledging the existence of these security concerns and issues, organizations will be more prepared to employ appropriate technology solutions necessary for protecting their BDS and the environment in which it operates. Risks associated with owning and storing data are likely to increase with the increase of volume, variety, and velocity. Thus, an efficient technology solution is necessary in ensuring a proper mitigation strategy is in place in managing risks and security breaches associated with big data.

Organizational Security Concern

Besides the security issues that require technological solutions, organizational security practices and culture should also be amongst the key factors when making decisions to adopt BDS. Organizational dimension can be described as characteristics that represent an

organization, such as company strategies, culture, structure and policies (Teo, Ranganathan, & Dhaliwal, 2006) . From an information security perspective, these characteristics may describe the organizational security practices and culture, security planning, security policy and risk mitigation strategies.

As in any other technology adoption practices, the role of top management in championing new technology adopted by their organizations is critical in ensuring smooth assimilation (Cruz-Jesus, Pinheiro, & Oliveira, 2019; Lai et al., 2018). A broad base of literature has also shown empirical support to the role of top management in motivating IT usage within organizations, e.g. (Herath et al., 2020). Thus, for the case of BDS adoption, and from the view of information security, it can be said that top management role is also important in promoting security culture and providing necessary support and security technology resources (Haeussinger & Kranz, 2017). Lack of top management support may hamper the efforts made by IS security professionals in protecting and securing organizational data and systems from functioning at optimum level.

A study on information security policy done by Mbowe et al. (2014), found that top management are more concerned with physical security as compared to IS security and left the process of securing data and systems solely to IT/IS staffs. If the top management places less importance on information security, especially when the organization is working with big data, it will be hard for them to ensure that the security controls put in place is aligned with the organization's security policy and culture. The top management needs to recognize the extent to which a breach in data security could affect their organization.

In addition, information security aspects must not be viewed as the sole responsibility of IS security professionals, instead, it must be embraced by all levels of employees in an organization. Hence, it is important for the top management of an organization to provide support in security management initiatives and promote security sense as part of organizational culture (Nasir, Arshah, & Ab Hamid, 2017). There have also been cases where security were considered at a later stage of adoption, as an afterthought, when organizations adopt new technologies (Bastos et al., 2018).

In an article by Praveenkumar *et al.* (2017), the authors suggest that most organizations view information security as an afterthought, especially during implementation of new technologies. In other words, security concerns and issues will only be investigated by the management when security incidents take place or are discovered. This tendency to consider security measures in isolation could cause potential harm to an organization, hence enforcing the need for top management and IS security professionals to be fully aware of the security concerns and issues associated with big data. As asserted by Thomas H. Davenport (2014), "big data changes not only technology and management processes, but also basic orientations and cultures within organizations". Therefore, organizational management and security practices and culture cannot be treated the same way as before the arrival of big data.

Security and Privacy Related Environmental Concern

Big data environment often involves the collection of data about individuals, especially by organizations that interact with consumers and through other business collaborations (Nguyen & Petersen, 2017). The data originates not only from within the organization, but are also mined from external data (Arfat et al., 2020). Thus, whenever these sensitive data are collected

and are being used within and across organization, the issue of privacy and confidentiality will emerge (Singh et al., 2018). As such, organizations need to consider its external environment that may affect the use of sensitive data in its big data initiatives.

One environmental factor that requires full consideration by organizations is the issue of rules and regulations. In protecting consumers' privacy and private data, many countries have introduced data protection act that aims to regulate the use of individual's personal identifiable information (PII) by organizations (Chua, Herbland, Wong, & Chang, 2017). Inevitably, organizations that work with big data will deal with PII even though they may have taken the steps to minimise individual identification through de-identification techniques and data anonymization (Demchenko, Ngo, Laat, & Membrey, 2014; Terzi et al., 2016). As the regulations that administers the use of data differs across countries, this will pose some challenges towards organizations wanting to leverage the potential of big data while at the same time having to abide with the legal provisions concerning the use of data (Duncan et al., 2018; Kshetri, 2014).

Another environmental factor that may concern organizations wanting to embark on big data initiatives is the issue of outsourcing and utilisation of third-party tools. In big data environment, there may be a need for organizations to outsource some part of the tools and applications that support data storage, sharing and access (Sivarajah, Kamal, Irani, & Weerakkody, 2017). According to Nguyen and Petersen (2017), most organizations are still unable to build and maintain a full-fledged big data environment in-house. Thus, this creates dependence on, for example, cloud service providers and other third-party tools vendors (Li & Gao, 2016; Simms, 2015). The need to outsource, although critical to creating and capturing value of big data, will create the need for a further consideration of security and privacy.

Evidently, there have been cases of security breaches that are associated with outsourcing practices (Benaroch, 2020). It implies that organizations may be unaware of how these third-party vendors may leave the door open to attacks. Organizations that decide to outsource a part of or the whole big data environment need to be aware of security best practices and work on decreasing the risks associated with outsourcing. This involves an awareness of which part of security control will be under the responsibility of the third-party vendor and those which are not. With this awareness, organizations will be more prepared to manage associated risks, especially those that are relevant to data security (Watson, 2019).

2.4 Conclusion

This chapter has presented a review on big data, BDS, big data adoption, and security concerns in relation to the use of BDS. The discussion provided on security and privacy challenges that are related to BDS was structured into three themes; technological, organizational, and environmental. These challenges and issues became one of the main motivations for this research – to study the security and privacy related factors that may affect organizational intention to adopt BDS. The following chapter will present the theoretical background that leads to the formation of the conceptual research model, which informs the research.

3. THEORETICAL BACKGROUND OF THE RESEARCH

This chapter informs on the theoretical background that forms the basis of this research. This research builds on a foundation of research in the areas of technology innovation, IT adoption, big data, and information security and privacy. Literature from a number of theoretical areas that inform the research were reviewed. Table 3-1 outlines the theoretical areas and briefly describe its relevance to this research.

Table 3-1: Theoretical Foundation of Security Determinants in the Adoption of BDS

Area	Relevance
Technology Innovation	BDS can be considered as organizational technology innovation
IT Acceptance, Implementation and Adoption	BDS are expected to exhibit adoption characteristics similar to other information technologies
Information Security and Privacy	BDS as in any other new technologies, may pose security challenges that may affect its adoption
Big data	Big data have a number of unique characteristics that may affect BDS adoption

In order to illustrate the above theoretical areas, the following section will provide an overview of the underlying theories in technology acceptance, adoption and innovation. Following it is a section that describes the technology adoption framework that was adopted for research – the TOE Framework. The discussion on other theoretical areas listed in the table above - big data and information security and privacy were provided in the earlier chapter.

3.1 Underlying Theories in Technology Adoption, Innovation, Acceptance and Use

Previous research on technology adoption, diffusion, and acceptance may aid in providing further understanding into factors that may affect the adoption of big data solution (BDS). Although the research only investigated security factors as determinants in BDS adoption intention, it was studied using the technology adoption lens. Thus, it is important to discern theories regarding how and why technology is introduced, diffused, and accepted as a basis for studying BDS adoption.

3.1.1 Technology Acceptance and Use

A vast amount of literature studying technology acceptance and use is available. From the literature, it can be seen that the bulk of research into technology acceptance and use focuses on examining the effect of user attitudes and beliefs, social norms, task-technology fit as well as self-efficacy (Agarwal & Prasad, 1998; Compeau & Higgins, 1995; Davis, 1989; Fishbein & Ajzen, 1975; Goodhue & Thompson, 1995; Rogers, 2003). Hence, the unit of analysis for this type of research are individuals. Examples of theories used in technology acceptance research are the Technology Acceptance Model (TAM) (Davis, 1989), and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2014). TAM is an intention-based model that aims to offer an explanation for the determinants of computer acceptance among users. Its general nature allows for the model to be applied in explaining user behaviour across a broad range of computing technologies while still remaining to be theoretically justified (Davis, Bagozzi, & Warshaw, 1989). In essence, TAM suggests that an individual's intention to use a certain technology is influenced by usefulness and ease of use of the technology itself. Venkatesh et al. (2003) proposed an extension to TAM through the introduction of Unified Theory of Acceptance and Use of Technology (UTAUT). This

model integrates elements from eight previous models including Theory of Reasoned Action (TRA), TAM, the Motivational Model, Theory of Planned Behaviour (TPB), the model of PC utilization, innovation diffusion theory, and the social cognitive theory, and a model that combines both TAM and TPB. Based on their findings, performance expectancy, effort expectancy, and social influence are found to be the direct factors in the intention to use a technology and that intention and facilitating conditions are direct factors in actual usage behaviour (Venkatesh et al., 2003). Based on the findings of previous research as shown above, it is important to acknowledge that organizational decisions to adopt a certain technology starts at the individual level. However, Tornatzky and Klein (1982) reminded researchers to avoid generalizing from the individual adoption process to the organizational innovation process, thus identifying the importance of using replicable and reliable measures. In essence, while individuals are known to be the drivers behind every organizational decision, this research seeks to model the security factors that may affect BDS adoption using organization as the primary unit of analysis. In the research process, certain parallels between individual acceptance and organizational adoption processes were also recognized.

3.1.2 Technology Innovation and Implementation

In understanding the reasons why and how a technology such as BDS was introduced and diffused in organizations, theories in relation to innovation and diffusion were also examined. The idea of information system implementation as a technological innovation was introduced by Kwon and Zmud (1987). Essentially, organizations will adopt technological innovations as part of a continuous process to improve their efficiency and effectiveness. As defined by Lyytinen and Rose (2003), “information systems innovations involve both a technological component (hardware and software) and an organizational dimension captured by such features

as new forms of work, business processes or organization methods". There are multiple reasons why organizations embark on a technological innovation process; amongst it is to ensure competitive survival and success (Swanson, 1994).

Swanson (1994) also suggests categorizing IT innovations into three subcategories. The author postulates that based on the type of innovation, different factors can have varying effects on an organization's adoption practices. Type I innovation was defined as innovations confined to the IT task, Type II innovation support the administration of businesses, and Type III innovations were embedded in the core technology of the business (Swanson, 1994). In this research, no focus was made as to which category of innovation the BDS falls into in its adoption by organizations. As BDS may serve different purposes according to organizational needs, this research considered an organization as an adopter or one having the intention to adopt BDS, when it falls into any of the three categories of innovation. Further, many of existing IT implementation research characterizes the adoption and use of new innovations by organizations as a linear process of moving through various stages. Rogers (2003) for example, proposes a five step process that organizations need to follow when choosing to adopt an innovation. The steps include knowledge acquisition, persuasion, decision, implementation, and confirmation.

Whilst, Swanson and Ramiller (2004) combined the elements identified by Rogers (2003) and came up with four processes; comprehension, adoption, implementation, and assimilation. Alternatively, Cooper and Zmud (1990) proposed a stage model for IT implementation that includes initiation, adoption, adaptation, acceptance, routinization, and infusion. Deriving from previous research on technology innovation and implementation as stated above, it can be

established that the organizational adoption of BDS may also exhibit the same linear process characteristics as other technological innovation.

As asserted by Kwon and Zmud (1987), research undertaken on IT implementation issues can be segmented into three categories. The first category is factors research, followed by process research, and political research. For factors research, it focuses on various issues that are significant in IT implementation effectiveness, such as individual, organizational and technological issues. Process research meanwhile, addresses social change activities (Kwon & Zmud, 1987). Under process research, there is a suggestion that implementation success relates to commitment to change, significant implementation efforts, extensive project definition and planning, and management if the process is guided by organizational change theories (Desanctis & Courtney, 1983). The third category of research, the political research, looks into the diverse assigned interest of organizational stakeholders and actors which may affect implementation efforts (Kwon & Zmud, 1987). It is believed that successful implementation depends on the ability to recognize and manage the diversity (Markus, 1983). In relation to this research, the category of research that it falls into is the factors research. This is shown in the research question that seeks to study the security technology, organizational security view, and security related environmental context factors that affects organizational intention towards adoption of BDS.

3.1.3 Technology Adoption

Kwon and Zmud (1987) defined technology adoption as the decision to invest resources that are required to provide technological change due to organizational needs (pull factor) or due to the technology itself (push factor). According to Rogers (2003), adoption of new technologies

and ideas, either within or across organizations, will begin slowly as only those people or organizations that are most innovative and risk takers will become early adopters. Others will observe the benefits derived by these early adopters, besides looking at the associated risk before beginning to adopt a certain technology. In the case of BDS adoption, the same phenomenon is being observed, as early adopters of the solution are technological firms such as Google (Kwon, Lee, & Shin, 2014) that are known to be innovators. Other organizations remain indecisive regarding BDS adoption due to various factors. This is evident from the results of studies conducted by market research firms (IDG Enterprise, 2014; NewVantage Partners, 2019).

There are various theories being applied by researchers studying technology adoption. Some of the theories are applicable to individuals as unit of analysis, for instance, the theory of planned behaviour (TPB) and there are those that cater to organizational/firm level of adoption. Due to the nature of this research that seek to study BDS adoption at organizational level, the research was specifically framed according to two theories/frameworks that are prominent in organizational technology adoption research (Oliveira & Martins, 2011). The two theories are the Technology-Organization-Environment (TOE) Framework (DePietro, Wiarda, & Fleischer, 1990) and Diffusion of Innovation theory (Rogers, 2003). Based on previous discussion on security concerns and practices in organization (Section 2.3) and more specifically security and privacy concerns in relation to BDS (Section 2.3.1), it can be said that various factors of security may have an effect towards organizational adoption of BDS.

Thus, the TOE framework which consists of three main contexts; technological, organizational, and environmental, is seen as one general framework that suits the research. The three contexts

include both internal and external factors that may affect technological adoption. The following section offers an explanation on TOE framework and how it was adapted for this research.

3.2 Technology-Organization-Environment (TOE) Framework

TOE framework was first introduced by DePietro, Wiarda and Fleischer in 1990 in their book chapter entitled *The Context for Change: Organization, Technology and Environment*. The book chapter explains in detail the whole process involved in innovation, including innovation development by innovators, and the actual implementation of the innovation within a firm (DePietro et al., 1990). This general framework in innovation studies, which represents a part of innovation process, describes three contexts that may influence the process of technological innovation adoption and implementation at firm level. The three contexts are technological context, organizational context, and the environmental context. The TOE framework has been used widely in IS research, with studies for different technology adoption and differing adaptation. Among recent studies that used the TOE framework as the theoretical basis for their research (either the TOE framework solely or by combination with other theories) are the studies by Park and Kim (2019), Herath, Herath and D'Arcy (2020), and Sun et.al. (2016). The above studies have shown that the framework has been empirically tested, thus making it an appropriate theoretical foundation for use in studies of IS innovation adoption and implementation. This framework has proven to be useful in considering factors involved in adoption of technological innovation, has broad applicability, and holds explanatory power (Baker, 2011).

The first context - the technological context, refers to both internal and external technologies relevant to the firm. Technology in this context may denote both equipment and processes.

According to DePietro, Wiarda and Fleischer (1990), the fit between the existing technology setting in a firm and the intended technology innovation will be the determinant in the decision to adopt technology innovation. Thus, the main emphasis is on how the adoption process may be influenced by technology characteristics themselves (Chau & Tam, 1997). The constructs that are originally presented in the TOE framework under the technological context are technological availability and technological characteristics (DePietro et al., 1990; Oliveira & Martins, 2011). Adaptation of the TOE framework in various technology adoption studies resulted in different constructs being used, amongst others being complexity and compatibility (adopted from Diffusion of Innovation theory) (Borgman, Bahli, Heier, & Schewski, 2013), relative advantage, complexity, compatibility, and security (Nguyen & Petersen, 2017), and, relative advantage, technological complexity, and data quality (Lai et al., 2018). For this research, the constructs used were *perceived complexity*, which refers to the technological complexity of ensuring security of BDS, and *perceived compatibility*, which refers to compatibility of current security technology of an organization to address the security concerns and threats of BDS.

The second context in the TOE framework is the organizational context. This context refers to multiple characteristics that represent a firm in general. The characteristics can be in the form of organizational strategies, culture, structure as well as policies (Teo et al., 2006). It may also refer to a measure that describes an organization, for example, the size of the organization, the scope of its business, and its managerial structure. DePietro, Wiarda and Fleischer (1990) stated that an organization itself is a "rich source". It consists of formal and informal processes and structures that in turn may have an effect in the adoption of technological innovation within the organization. Further, availability of slack resources in an organization and the quality of human resources also contributes to the organizational context of this framework (Rosli, 2012).

Thus, it can be said that the organizational context of TOE framework represents a set of firm/organizational level characteristics that will have an impact on decision making in relation to any technological diffusion and infusion. These characteristics may serve as constraints in adoption or they may also be the facilitating characteristics in adoption of new technology for organizations (Oliveira & Martins, 2011; Teo et al., 2006).

Similar to the first technology context, organizational context also saw different constructs being used or added to the original constructs introduced by DiPietro et al. (1990). The constructs that are originally listed under organization are as follows: formal and informal linking structures, communication process, size, and slack resources (DePietro et al., 1990). Because TOE is being used to understand different IT adoptions, constructs used by researchers under the organizational context are adapted accordingly to suit the needs of their research. A study on EDI adoption by Kuan and Chau (2001) used perceived technical cost and perceived technical competence as constructs for the organizational context. Other example of constructs that were used include top management support, IT infrastructure/capabilities, and financial readiness (Lai et al., 2018), and firm size, top management support, and IT expertise of business users (Borgman et al., 2013). The constructs that were adapted for this research are, *top management support*, *information security culture*, and *organizational learning culture*.

The TOE framework environmental context refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealings with the government" (DePietro et al., 1990). This context fundamentally implies that in order for organizations to adopt new innovation or technology, there will be influences emanating from the environment in which the organization operates. These external factors may include organization's clients, suppliers, its market competitors, government regulations, and other

related external pressure and forces. These external entities may become the constraints in technology adoption, and some may also provide opportunities to organizations planning to adopt a certain technology. For instance, having consultants and other providers of technology services may increase an organization's intention to adopt technology and nurtures innovation (Baker, 2012). In addition, one external factor that may provide both opportunities and constraints to technology adoption is government regulation. Regulations set by governments such as data privacy requirements may hinder certain organization from using a certain technology that utilizes customers' information for marketing purposes. Regulations that are too strict may also be detrimental to technology adoption in organizations, especially when a regulation is imposed for certain industries (Baker, 2012).

Like both technological and organizational contexts, environmental context also saw its constructs being added or adapted to suit a researchers' need. Previous studies have seen differing factors being studied under environmental context, for instance, competitive pressure was postulated to positively influence CRM evaluation and adoption (Cruz-Jesus et al., 2019). Whereas others like Borgman et al. (2013), postulate that competition intensity, and regulatory environment affects the intention of organizations to adopt cloud computing. In keeping with the above suggestions, this research included *regulatory concerns* (security and privacy related regulations) as one of the constructs under environmental context. Besides regulatory concerns, *risks of outsourcing* were also identified from the systematic literature review conducted as having an effect towards the adoption process, thus it became the second construct under the environmental context.

As discussed earlier, in existing empirical studies that adopted the TOE framework to study the assimilation and adoption of different types of IT innovation, researchers have used

differing constructs besides the ones originally presented by DePietro, Wiarda and Fleischer. Each of the three contexts received different treatments to satisfy specific research needs. In principle, this shows that researchers agreed with the three main contexts introduced, but assumptions were made by these researchers that different technologies require different measures and unique sets of constructs. Since innovations vary in nature, it is safe to conclude that these innovations will be influenced by different factors. Besides the type of innovation, other contexts that may influence technology adoption also vary according to national/cultural aspects, and industries (Baker, 2012).

These factors are amongst the reasons why the TOE framework saw different factors or constructs being applied by researchers in each of its three contexts: the technological, organizational, and environmental contexts. The freedom to vary the constructs and its high adaptability are amongst the reasons why the TOE framework remains widely used in technology adoption research.

3.3 Conclusion

This chapter has presented the theoretical background of the research. In principal, a deliberate decision was made to select the TOE Framework as the main theoretical foundation for this research. This is due to the suitability of its three main contexts to classify the seven constructs derived from the earlier literature review process carried out to identify the security and privacy issues associated with big data (as reported in Article 1). The next chapter will present the research methodology adopted for the research and the conceptual framework depicting the main stages of the research.

4. RESEARCH METHODOLOGY AND CONCEPTUAL FRAMEWORK

This chapter will introduce the research methodology adopted by the research. The chapter will then present the overarching conceptual framework of the thesis and subsequently present the research questions.

4.1 Research Methodology

As mentioned briefly in Chapter 1, the research methodology used for this research is sequential explanatory mixed-method approach. Mixed-method approach is a type of investigation with a deliberate mixture of both quantitative and qualitative study which are used in a single research study (Venkatesh, Brown, & Bala, 2013). According to Creswell and Clark (2018), a mixed-method approach aims to provide a more complex understanding of a phenomenon being investigated, especially in situations where a single approach of doing research may not alone be able to provide the required level of understanding.

In a mixed-method approach, there are three basic designs that can be adopted depending on the research questions and aims. The three types of design are; convergent/concurrent, sequential, and embedded (Klassen, Creswell, Plano Clark, Smith, & Meissner, 2012). This research adopted the sequential design which allows for one data collection activity to be built based on the results of another data collection activity (Klassen et al., 2012). More specifically, this research used the sequential explanatory mixed-method approach where a qualitative study was conducted in the second phase of data collection to provide further explanations on the results of the first stage of quantitative data collection. Amongst the advantages of sequential

explanatory mixed-method design are; it is straightforward, and it provides researchers with the opportunities to explore in detail the results gathered from the quantitative study (Ivankova, Creswell, & Stick, 2006). In essence, sequential explanatory approach aims to have qualitative data that will assist in clarifying the initial quantitative result (Creswell & Clark, 2018). This research follows the sequential explanatory mixed-method design procedures suggested by Ivankova et.al. (2006).

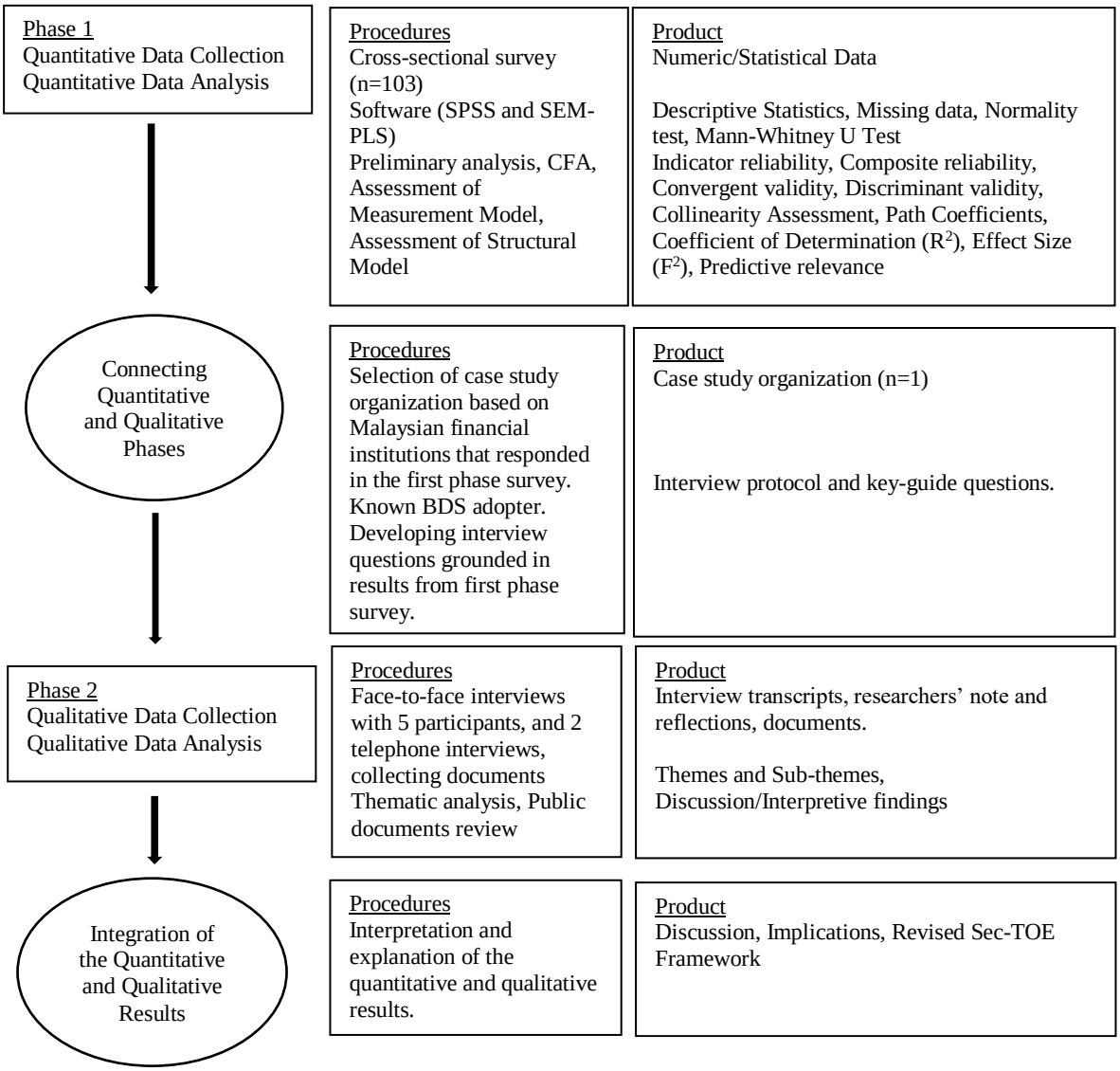


Figure 4-1: Visual Model for the Study's Sequential Explanatory Mixed-Methods Design Procedures

The explanations on the specific data collection techniques, analysis procedures, outcomes of each stage of the research, and integration of both stages are detailed in Chapter 10 (Article 6). The procedures involved were also incorporated in a visual model for ease of comprehension (Figure 4-1).

4.2 Conceptual Framework of the Thesis

There are several definitions of a conceptual framework, but the one that best describes the conceptual framework presented in this chapter is the one suggested by Miles and Huberman (2014); a conceptual framework is "a visual or written product, one that "explains, either graphically or in narrative form, the main things to be studied—the key factors, concepts, or variables—and the presumed relationships amongst them" (Miles & Huberman, 2014).

In other words, the conceptual framework models the main areas of interest for the researcher and provides an outline of how the study will be carried out. Hence, the conceptual framework presented in this chapter is meant to provide an overview of the main stages of the research, as well as show how the six original articles written by the researcher are linked to one another. It is also intended to show how these articles fit in towards forming the 'bigger picture' of the research problem.

The conceptual framework depicting the main phases of this research is illustrated in the following Figure 4-2. For visualizing the procedures involved, the steps are divided into 3 main stages in the conceptual framework: 1) exploration, 2) analysis, and 3) outcome.

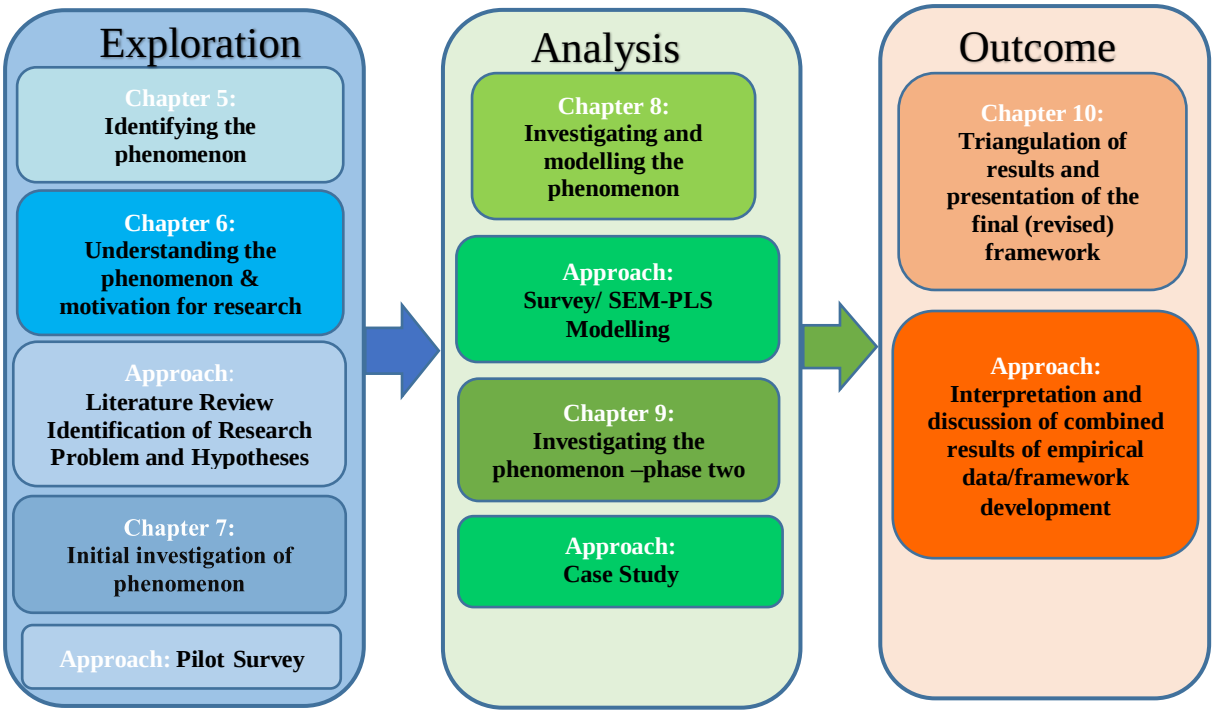


Figure 4-2: Conceptual Framework Depicting Main Phases of Research

The *exploration* stage involves the process of understanding and determining the phenomenon of interest for this research. Besides presenting the motivation of the research, the initial introduction to the main research problems were also made during this exploratory stage. This stage also involved an initial investigation of the phenomenon of interest during which a preliminary pilot study was conducted.

The *analysis* stage comprised two phases of empirical studies. The first phase involved investigating and modelling the phenomenon of interest. Next, the results generated from the first phase were used as a link to the second phase of study. Both phases studied the same phenomenon, however using different data collection and analysis methods. The results generated from both these phases were then integrated to form the outcome for the next stage. The third and final *outcome* stage is where the final results of this research is presented, through triangulation of results, and a revised conceptual model.

As this research adopts a sequential explanatory mixed-method approach, two methods were used for data collection (questionnaire survey for the first phase of study and a single organizational case study for the second phase). The second phase of the study (case study), builds on the findings and insights gained from the first phase of data collection. These findings were then shared with interested parties by means of six peer reviewed publications (5 published, 1 submitted for publication). The feedbacks received from the reviewers and other interested parties were then incorporated into subsequent stages of the research. The following is an elaboration of the three main stages and its components.

4.3 Stage 1: Exploration

This stage began on the simple premise of understanding the security and privacy issues related to big data and how these issues may impact organizational intentions to adopt big data solutions (BDS). During the early stage of this research, the main assumption of the researcher was as follows; while big data is gaining momentum in its acceptance across industries and organizations, there still remain privacy and security related issues in big data solutions that may deter organizations from fully embracing BDS.

This assumption was supported by the findings of several big data surveys and empirical research, which listed security and privacy related concerns as one of the main factors deterring adoption (Nguyen & Petersen, 2017; Raguseo, 2018; Sans Institute, 2015; Yadegaridehkordi et al., 2018). This realisation prompted the researcher's interest in exploring the possible security and privacy factors that may affect BDS adoption intentions in organizations. The *exploration* stage was divided into three parts:

4.3.1 Identifying the Phenomenon

The aim of this component in the exploration stage is to identify the security and privacy issues related to big data and to classify them accordingly in a classification framework. To achieve this aim, literature search was conducted on Information Systems' top journals and top citation indices using the term "big data" as the keyword. The results obtained were screened in stages and only relevant articles were retained for content extraction.

The review process identified the security and privacy related issues described in the articles and finally, these issues were categorized under three main headings: *technological factors in security, organizational factors in security,* and *environmental factors in security*. Hence, the research question for this thesis is centred around identifying different themes or main security and privacy factors that are normally associated with big data. Therefore, this leads the researcher to the first research question which is:

Research Question 1: What are the main themes related to big data's privacy and security issues?

Six themes were identified as the main security and privacy issues; *security and privacy technological complexity, security and privacy technological compatibility, organizational learning culture and competencies, information security culture and top management support, privacy regulatory concern* and the final theme was *risks in outsourcing and use of third-party tools*. The identification of these six themes were then used for further understanding of the phenomenon and motivated the subsequent stages of the research. The complete findings of this stage are published in Article 1.

4.3.2 Understanding the Phenomenon and Motivation for Research

The next part of the exploration stage was meant to set the boundaries and scope for the rest of the research process. The overall research design was presented during this stage and a theoretical framework with its associated hypotheses was introduced as a guiding framework for the research. Based on the findings of Article 1 and after a further review of literature, TOE framework (DePietro et al., 1990) was found to be a suitable framework for application in this research as it covers the three main contexts of technological, organizational and environmental related issues commonly studied in technology adoption literature. The researcher decided to focus on the security and privacy determinants in BDS adoption in order to gauge the effects that these security factors may have on adoption intentions. Thus, the main research framework was named the Sec-TOE framework, to highlight the security-focused factors of the framework. This initial exploration, understanding and research boundary setting led to the identification of the following main objective of this research:

1) ***To provide a conceptual security based BDS adoption framework as a guide for organizations planning to embark on big data initiatives.***

And the following two ancillary objectives;

1) ***To examine the security determinants by focusing on the influence that various security technologies, organizational security view and security related environmental factors have on BDS adoption.***

2) ***To ascertain the security and privacy-related considerations made by organizations in the process of BDS adoption.***

The theoretical research framework (Sec-TOE), a brief explanation of the sequential explanatory mixed-method approach as the methodology for the subsequent stages, and boundaries of the research were all reported in Article 2.

4.3.3 Initial Investigation of Phenomenon

The third part of this *exploratory* stage led to the publication of Article 3. For part three, after considering the methodology setting in Article 2, the researcher developed a survey instrument for use during the first phase of data collection. In order to check for the validity of the survey instrument and to generate initial descriptive findings, a preliminary study was conducted using an online questionnaire platform, *Qualtrics.* The target respondents for this preliminary study were members of the New Zealand Information Security Forum (NZISF). NZISF is a special interest group whose members are mainly information security practitioners in organizations throughout New Zealand.

Data analysis for this preliminary stage was conducted using statistical software- SPSS. Descriptive findings of this stage were then divided into results for adopters and non-adopters of BDS. From the generated results, it was found that several factors have differing influences on the intention to adopt between the two categories of adopter organizations. Hence, the research question prompted by this part of the research namely:

Research question 2: How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption among adopter and non-adopter organizations?

Amongst the main findings of this pilot stage are organizations which are classified as adopters are positively affected by *perceived compatibility*, *top management support*, *information security culture* and *organizational learning culture*. Whilst, the non-adopters appear to be negatively affected by two factors; *perceived complexity* and, *risks in outsourcing*. The full results of this preliminary study conducted using survey methodology techniques were reported in Article 3.

4.4 Stage 2: Analysis

This stage includes two major data collection phases carried out to provide support for hypothesis testing and the research framework. The first phase of data collection was quantitative in nature (cross-sectional survey) and the second phase was a qualitative study (single case study).

4.4.1 Investigating and Modelling the Phenomenon

After gaining initial descriptive results from the previous stage, all comments and feedback received were then used to update the survey instrument. The final questionnaire was then administered to public listed organizations in both New Zealand and Malaysia. The survey was administered employing two methods; mail survey and online survey (*Qualtrics*). In total, 103 responses were received (44 from New Zealand and 59 from Malaysia).

Stratified random sampling was used for this first-phase survey. The stratums were divided based on industries that have the highest prospect of having big data; e.g. finance, telecommunication, health, and retail. Primary unit of analysis was *organization*. At this stage, the researcher made the decision to use SEM-PLS as the main analysis tool after initial statistical evaluation made on the collected data (using SPSS). This first phase of analysis was meant to address the following research question:

Research Question 3: How do technology factors in security, organizational security view, and security-related environmental factors encourage/discourage organizations' big data solution adoption?

This third research question is very similar to research question 2. However, the main difference between the two is that answers for research question 3 were derived by analysing the collected dataset (N=103) wholly, without categorizing the respondents into adopters and non-adopters. After conducting an examination of potential biases that may be contributed by use of the survey methodology (where no statistically significant biases were found), the researcher concluded that the use of pooled datasets that combined responses from both adopting and non-adopting organizations was sufficient to produce a PLS model with greater predictive accuracy.

The resulting PLS model shows the path significance of each construct and the predictive accuracy of the model. Five factors were found to be statistically significant; *perceived complexity*, *top management support*, *information security culture*, *outsourcing risks*, and *security/privacy regulatory concerns*.

The analysis of the assessments done on the measurement and structural model, the resulting PLS model, and the full results were reported in Article 4.

4.4.2 Investigating the Phenomenon – Phase Two

This phase of the data collection was a case study involving a public listed bank in Malaysia. The participants of this case study were employees of the bank who either had direct knowledge of the bank's technology adoption processes, the bank's information security procedures or were the direct users of the bank's BDS. Besides the interview transcripts, secondary documents were also reviewed during the preparation of this analysis stage. Three main themes and ten sub-themes were identified from the thematic analysis conducted. This phase was meant to complement the results derived from the earlier survey. The link between the earlier survey and this case study was created through the identification of main themes which were grounded in the main theoretical framework used during the earlier survey namely the Sec-TOE framework. This connection was also made during development of key interview questions (interview protocol) which was grounded in the results of the earlier survey. Hence, the research question posed for this phase is:

Research Question 4: Do organizations consider security-related factors during BDS adoption and if so, what considerations are made?

The results of the thematic analysis carried out on data collected during this phase were reported in Article 5.

4.5 Stage 3: Outcome

This final stage aims to present the summarized findings of the whole research and thus present the revised conceptual model of security determinants in big data solutions adoption (Sec-TOE Framework).

4.5.1 Triangulation of Results and Presentation of the Final Conceptual Model

For this final phase, a triangulation/integration of both quantitative and qualitative data was made in order to derive the final conceptual model. Interpretation and explanation of the quantitative and qualitative results were carried out resulting in a final discussion of the implications of the research. Following on from this, the fifth research question was formulated as follows:

Research Question 5: What recommendations on security-related determinants can be introduced for organizations adopting big data solutions?

The presentation of the final conceptual model and the analysis of the outcome is reported in an article that is being submitted for publication to a journal as Article 6. The next section explains how these six articles are linked and how they fit within the conceptual framework.

4.6 How the Articles Are Linked and Fit Within the Conceptual Framework

While carrying out this research, six original articles were written based on the stages identified earlier in the conceptual framework presented in this chapter. Out of the six articles, five have

been published, while the final article has been submitted for publication and is presently awaiting notification of acceptance (as of Jan 2021).

As part of this thesis, it is therefore essential to describe how these articles are connected to one another as well as how the articles fit within the conceptual framework. Figure 4-3 illustrates the connection of the articles and how these articles fit within the three stages of the conceptual framework.

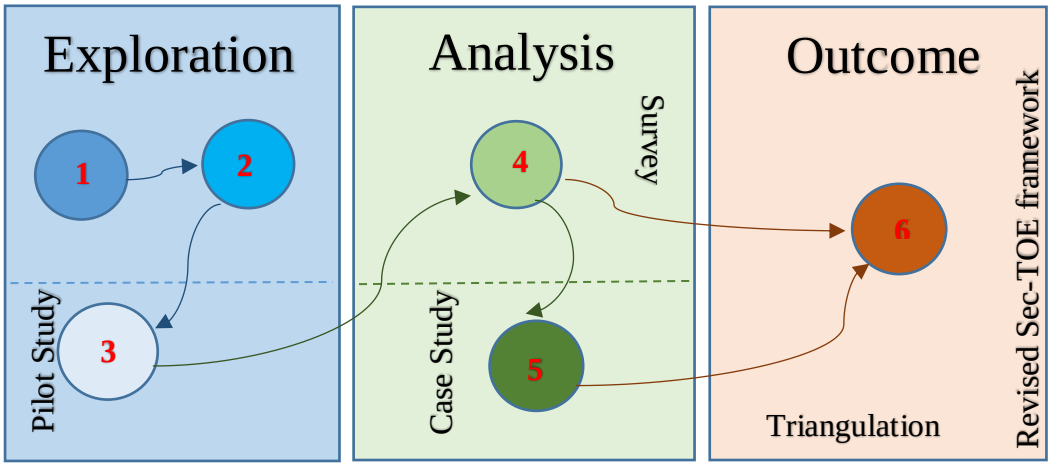


Figure 4-3: How the Articles Are Connected and Fit within the Conceptual Framework

4.6.1 The Original Articles

The first article (Article 1 – "*Technological, Organizational, and Environmental Security Issues of Big Data: A Literature Review*") was submitted to the Conference on Enterprise Information Systems (CENTERIS2016). The proceeding of CENTERIS2016 was published in Procedia Computer Science volume 100. This exploratory article presented a literature review of the security and privacy issues surrounding big data. The issues derived from content extraction/review as reported in this article were then used as the security-related factors in

BDS adoption for the theoretical framework introduced in Article 2. It also forms the basis for theoretical research model development in subsequent stages.

Article 2, *"Sec-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption"*, was presented and published in the Proceedings of Pacific Asia Conference on Information Systems (PACIS2015) as a research-in-progress article. This article introduced the overall research background, research plan, research framework, hypotheses as well as the selected research methodology. The theoretical research framework and the hypotheses were based on a comprehensive literature review conducted on the issue of security and privacy of big data, big data adoption, within the domain of general technology adoption.

Next, Article 3, "Adoption of Big Data Solutions: A Study on its Security Determinants using Sec-TOE Framework" was published in the Proceedings of Conference on Information Resources Management (CONF-IRM2016). The content includes a description of the preliminary study conducted to test the survey instrument developed to measure the hypotheses initially presented in Article 2. The descriptive results of this preliminary study were also included in this article.

Article 4, "An Implementation of Sec-TOE Framework: Identifying Security Determinants of Big Data Solutions Adoption" was published in the Proceedings of Pacific Asia Conference on Information Systems (PACIS2018). This article provides answers to the third research question by reporting on the results of the first phase cross-sectional survey. A PLS model that shows significant and non-significant constructs' path towards the endogenous variable was also presented.

The second phase of the study resulted in Article 5, titled "Security Considerations on Big Data Solutions Adoption: Lessons from the Case Study of a Banking Institution". This article was accepted for presentation at the Conference on Enterprise Information Systems (CENTERIS2019) in October 2019. The article was then published in *Procedia Computer Science* series (Volume 164). This being the second article from the analysis stage, presents the results of the case study conducted on a Malaysian banking institution. The results from this study are meant to complement the results of the first quantitative phase.

Finally, Article 6, "Security Determinants in the Adoption of Big Data Solutions: A Mixed-Method Approach" was submitted to Asia Pacific Journal of Information Systems (APJIS). This concluding article presents the overall research by explaining the mixed-methods approach, results of both studies, and integration of results which then led to the development of a revised Sec-TOE framework.

All articles were presented in their entirety as in the published version except for the addition of some linking sentences/paragraphs to smooth the transition from one article to the next. Article 6 has an extra sub-section which was not present in the published version (due to page limits). The numbering of figures and tables were also adjusted to accord with the chapters in the thesis. These articles are included in this thesis forming chapters 5, 6, 7, 8, 9 and 10 respectively.

4.7 Conclusion

This chapter presented a brief discussion on the research methodology adopted for the research. An explanation on sequential explanatory mixed-method approach was provided; in addition

to a presentation of the conceptual framework dah depicts the three main stages of the research. The processes involved in each stages were also discussed in detail. Each articles were individually described in the last section of this chapter. Primarily, the articles show the progression of the research work starting from its exploratory stage up to the outcome stage. Comments and reviews received for each article were considered in improving the research design and reporting of subsequent research phases/stages. The following chapters consist of the original published articles (and an article submitted for publication) that taken together address all research questions presented in this chapter.

5. Technological, Organizational, and Environmental Security Issues of Big Data: A Literature Review (Article 1)

5.1 Introduction

Big data is a term that frequently appears in current business and academic discussions on recent technology trends. In publications, this term is rarely discussed without the inclusion of its unique characteristics; the 3Vs. The first 'V' refers to 'Volume', which describes large amount of data, the second 'V' is for 'Variety'- different types and sources of data and the final 'V' refers to 'Velocity' – the speed of data transfer and creation (Bansal, Kaur, & Aggarwal, 2014). Else, other V's have also been described as forming the unique characteristics of big data, such as 'Value' and 'Veracity' (Martin, 2015). These characteristics notably differentiate big data from the traditionally known methods used to capture, store, and analyze data. At present, big data is gaining greater attention due to increasing number of connected devices that generate very large amount of data. With proper use of big data technologies and applications, organizations will be able to exploit these data and transformed it into valuable information.

While the benefits of big data may reach diverse functions in organizations and individuals' life in digitized world, this extent of reach however, introduces far greater exposure to security and privacy risks. Although it is undeniable that big data sources may be utilized to derive better insights (Dhar & Mazumdar, 2014), but the underlying security and privacy concerns remains. These concerns may possibly be amplified by big data's volume, variety and veracity when deploying system infrastructure in supporting big data applications (Alshboul,Wang, &Nepali, 2015). Organizations today are already confronted with overwhelming tasks of protecting their information assets, hence to some organizations; the idea of having big data

applications deployed will invite further security issues and larger number of breaches. In fact, security and privacy issues have been cited in some big data survey done by technology providers and market research companies as one of the hindering factors in big data adoption (Gartner Inc, 2014; IDG Enterprise, 2014; Sans Institute, 2015).

Even though these issues have been reported multiple times as one of big data's adoption hindering factors, the specific security and privacy related issues that is of concern to organizations considering big data adoption are rarely discussed in publications. This study therefore intends to derive the possible security and privacy issues that may be influencing big data adoption by reviewing literatures in information systems domain. The following sections proceed as follows: section 5.2 briefly presents the motivation/objectives of the study and section 5.3 described the research methodology. The following sections present the findings of the literature review by classifying it into three contexts (section 5.4, 5.5, 5.6). The final sections draws a conclusion and provides future research direction.

5.2 Motivation, Scope and Objectives

Existing scholarly literature on big data are written from different perspectives to highlight the various application of big data and its associated challenges in today's data driven era. Majority of literature on big data at present can be grouped into the following categories: big data overview, big data processing algorithm, big data applications, big data infrastructure and big data security, privacy and trust (Chen et al., 2016). The largest number of publication can be found under the big data overview category, where scholars provide a general overview of big data, its challenges, the framework, techniques and technologies as well as other issues related to big data and its future direction in research. Examples of publications that fall under this category are those written by Chen and Zhang (Chen & Zhang, 2014), an article that discusses

on big data's impact on privacy, security and consumer welfare by Kshetri (Kshetri, 2014) and an article by Abbasi et.al. (Abbasi et al., 2016) that critically discuss the research agenda for big data research in information systems (IS).

This study chooses to add to the body of knowledge in the area of big data adoption/application and its associated security and privacy related concerns. While there are numerous publications that highlight the application of big data, the ones that specifically present the relation between security and privacy issues in big data adoption are still fragmented and scarce. Most discussion on security and privacy issues of big data exist as a sub-section in articles that surveyed big data challenges and opportunities in general.

Hence, this study aims to contribute to big data domain by conducting a literature review on big data's security and privacy related concerns and to present on how these security concerns may affect big data adoption by organizations. The main objectives of this study are: 1) To identify studies that discuss on security and privacy concerns of big data, and, 2) To categorize the security and privacy concerns/issues found in the articles into a classification framework (TOE).

5.3 Methodology

References to big data, analytics, big data technologies and certain combination of these terms can be found in most popular publication - in both online and physical form of publication. For the purpose of this study, the initial literature search was made on top IS academic journals. The IS journals selected are the eight leading journals under the Senior Scholars' Basket of Journals; European Journals of Information Systems, Information Systems Journal, Information Systems Research, Journal of Information Technology, Journal of MIS, Journal of

Strategic Information System, Journal of The Association of Information Systems and MIS Quarterly. The keyword used was "big data" and the years of publication were restricted to those published in 2010 to February 2016. This initial search yielded only 9 relevant articles.

Second phase of literature search was then made on the Web of Science platform, specifically using two citation indices, the Science Citation Index (SCI) and Social Science Citation Index (SSCI). This search retained the same keyword (big data) and the timeframe of publication (2010 – 2016), while the Web of Science categories of articles were restricted to 'computer science and information systems'. The search returned a total of 516 articles and after refining the search to include only articles and reviews written in English, it went down to 439. Next, taking into account that new ideas and theories are commonly presented in academic conferences, a search was also made on leading information systems conference proceedings. Association for Information Systems (AIS)'s and its affiliated conferences were chosen and as a result 9 articles were found (including 4 from AIS journals). In total, 457 articles were considered for final assessment. The final assessments were then conducted based on the following criteria:

- The article falls under 'overview' or 'security and privacy' category. (Categories based on Chen et.al. 2016 (Chen et al., 2016)).
- Articles under 'overview' category must include contents on security and privacy.

Based on the selection criteria, 44 articles were found to fall under the 'overview' category and 25 articles under 'security and privacy'. The articles under 'overview' category were then checked for any inclusion of security and privacy content which resulted in 25 relevant articles. Security and privacy articles were also checked for its relevance in supporting the aims of this study, and 18 articles were found to have contents of high relevance. At the end of this process,

43 articles were identified for content extraction. Table 5-1 summarized the results of the literature search.

Table 5-1: Summary of Results According to Categories

Category of big data articles	Number of Studies	Publication & References
Big data overview	25	Journal of AIS (Abbasi et al., 2016), Business & Information Systems Engineering (Buhl & Heidemann, 2013) (Jarke, 2013), Journal of Information Technology (Bhimani, 2015) (Markus, 2015), Decision Support System (Chang, Kauffman, & Kwon, 2014), MIS Quarterly (Chen & Storey, 2012) (Goes, 2014), Mobile Networks and Applications (Chen, Mao, & Liu, 2014), Journal of the Association for Information Science and Technology (Ekbia, Bowman, & Weingart, 2015) (Frické, 2015), Foundations and Trends in Information Retrieval (Gurrin & Smeaton, 2014), KSII Transactions on Internet and Information Systems (Jeong & Ghani, 2014), Journal of Strategic Information Systems (Loebbecke & Picot, 2015), IBM Journal of Research and Development (Malik, 2013), IT Professional (Miller & Mork, 2013) (Kemelor, 2015), Information Sciences (Philip Chen & Zhang, 2014), Communications of the Association for Information Systems (Phillips-Wren, Iyer, Kulkarni, & Ariyachandra, 2015) (Shim, French, & Jablonski, 2015) (Watson, 2014), MIS Quarterly Executive (Martin, 2015), IEEE Network,(Yin, Jiang, Lin, Luo, & Liu, 2014) (Fang, Zhang, Wang, & Daneshmand, 2015), IEEE Transactions on Services Computing (van der Aalst & Damiani, 2015).
Big data security and privacy	18	Ad Hoc Networks (Chang, 2015), Security and Communication Networks (Chen, Liang, & Wang, 2015), Tsinghua Science and Technology (Dong et al., 2015), IEEE Security and Privacy (Eckhoff & Sommer, 2014), Proceedings of Pacific-Asia Conference on Information Systems 2013,(Saenz, Chang, Kim, & Park, 2013), Information Security (Goodendorf, 2013) (Lane, 2014) (Ranum, 2014) (Richardson, 2013), Information Systems Frontiers (Hota, Upadhyaya, & Al-Karaki, 2015), Network Security,(Lafuente, 2015), IEEE Network (Lu, Zhu, Liu, Liu, & Shao, 2014), Thirty Fifth International Conference on Information Systems (Mennecke et al., 2014), IT Professional (Perera, Ranjan, Wang, Khan, & Zomaya, 2015), Conf-IRM2015 Proceedings (Perreault, 2015), IEEE Transactions on Multimedia (Samuel et al., 2015), Information Sciences (H. Wang, Jiang, & Kambourakis, 2015), Twenty-First Americas Conference on Information Systems (Alshboul, Wang & YongNepali, 2015).

For further review of the articles, an inductive categorization will be used in classifying the contents into three contexts; technological, organizational and environmental (TOE). These contexts are part of an organizational level technology adoption framework, known as TOE Framework (DePietro et al., 1990). The reason for this classification is to provide a basis for further research on how technological, organizational and environmental security issues of big data may influence its adoption process by organizations. As security and privacy issues may encompass various factors other than its technological aspects, TOE Framework is deemed suitable for this classification purpose.

5.4 Security and Privacy Issues in Technological Context

Technological context refers to both internal and external technologies relevant to organizations (DePietro et al., 1990). Hence, technology in this context may include current practices, equipment and processes (Oliveira & Martins, 2011). Most of the reviewed articles include a discussion on how big data creates technological-related security and privacy issues, where some of the issues were associated to big data's unique characteristics (Alshboul Wang&YongNepali, 2015). Each of these characteristics will pose certain security concerns that require a strong security solution and mechanisms in ensuring the confidentiality, integrity and availability of data.

The sheer volume of data collected and created in a typical big data environment is one the factors inviting security issues. Accordingly, new and improved security tools and mechanisms are needed in order to provide effective protection towards data. However, in an article by Adrian Lane (Lane, 2014), the author suggests that "many security professionals who encounter big data environments for the first time don't understand why security is a big issue". This shows that at present, the degree of difficulty and impact of big data related security issues

are yet to be realized by security professionals. The same tools and techniques used to provide security to a relational database for example, will no longer be sufficient in a big data environment (Chen et al., 2014; Lane, 2014). A typical multi-node architecture of a big data environment, coupled with the volume of data will naturally outrun the capacities of any standard security products.

In another article that proposes a framework for secure sensitive data sharing for big data platform, the inadequacy of existing security technology is also discussed. By looking at data sharing and privacy protection issues, the authors noted that existing technologies did not take into account the whole process of data security life cycle hence endangering a big data environment (Dong et al., 2015). In addition, Chen and Zhang (Chen & Zhang, 2014) asserts that data security issues for big data application are somehow "awkward" for a number of reasons, among it is the protection approaches required are closely related to the size of big data – larger size of data means larger protection coverage needed. Due to the distributed nature of a big data environment, threats arising from networks may also magnify the problems in protection, resulting to a heavier workload for security functions (Chen & Zhang, 2014). In essence, the 'volume' characteristic of big data will pose a challenge to existing security technologies and solution. As described above, one the key challenges is to provide security technologies and solution that are able to scale to the large size of data sets and distributed nature of big data (Demchenko et al., 2014).

The speed in which data are being created and the speed of how it should be analysed and acted upon; may also pose some security threats. In a big data environment, data is being generated in an unprecedented rate, either in batch, real time/near time, or streams (Demchenko et al., 2014). Many organizations are currently generating high frequency data and this may create

difficulties in maintaining data protection. In presenting a new secure transmission method for big data, Chen et.al. (Chen et al., 2015) highlights that collection and transmission of data through any communication networks will essentially introduced critical requirements for security. The same concern is reiterated by Dong et.al (Dong et al., 2015) by providing some examples on how security issues may appear during rapid transmission of sensitive data. For instance, during the phase of data creation, a rapid transfer of data streams from owner's local server to a big data platform could create security issues which may lead to the loss of sensitive data. During the rapid transmission, creation and processing of data, an organization must ensure that data are aggregated or anonymized to prevent any access to personal identifiable information. Strict control and measures must be readily available during these transmissions of data to alleviate risks and errors (Chang et al., 2014). Rapid frequency of data creation and processing will also create issues when there is a lack of security capabilities in securing data storage particularly during peak data traffic (Kshetri, 2014). Rapid data flows will also increase the need to have a security technology with the ability to screen and audit access while at the same time protecting data stored across repositories. It is now apparent that 'velocity' of data in a big data environment amplifies security complications commonly found in any traditional data environment, and at the same time produces new issues that requires special treatment (Wang et al., 2015).

Another unique characteristic of big data is the various sources and types of data that are collected and stored in a big data environment. The 'variety' of data often originates from structured, semi-structured and unstructured data. Thus far, most organizations are familiar with the security mechanisms that are applicable in protecting structured data, but with the inclusion of unstructured data, the experience may be lacking (Kshetri, 2014). Samuel et.al. (Samuel et al., 2015) states that variety of data posed security and privacy challenges for

organizations and to “compose a unified, broad privacy policy” will be unsuitable. Secure access management will also be a problem when the data derived are stored in data repositories that reside in distributed location across a big data environment. Wang et.al. (Wang et al., 2015) emphasizes that the variety of data will require a cumbersome tasks of providing different restrictions for access and security policy that suits each sources of data. Consequently, it will be difficult to balance the appropriate security mechanisms needed with the tasks of extracting value from the data.

The variety nature of big data may also create new challenges in data encryption. According to Chen et.al. (Chen et al., 2014), high diversity big data demands for newly developed efficient cryptography approaches which could not be met by previous encryption approaches. The authors then highlight on the requirement for an effective security schemes (safety management, access control and safety communications) for all types of data; from structured to unstructured. At present, it is understood that existing mechanisms for the protection of unstructured data is still in its growing phase and data governance issues are still not fully addressed. Without effective input validation, identifying malicious data sources may prove to be an overwhelming process. Hence, Malik (Malik, 2013) proposed for organizations planning to launch big data initiatives, to consider the requirements of producing liable mechanisms for security and privacy, including defence in depth for each type of data.

As illustrated above, organizations that are already a part of big data initiatives or are planning to jump into big data bandwagon, are faced with numerous security and privacy issues in relation to infrastructure, processes and protection mechanisms. To summarize, all the technological challenges posed by big data, may reflect the complexity in providing effective protection to big data environment. Whereas, the level of preparedness of organizations in

embracing all challenges that comes with big data, may be attributed to the organizations' perceived compatibility of their current security mechanisms with those required by big data. It is thus interesting to see whether these two factors, 1) Complexity and 2) Compatibility have any influence on organizations planning to adopt big data.

5.5 Security and Privacy Issues in Organizational Context

Organizational context can be described as characteristics that represent an organization, such as company strategies, culture, structure and policies (Teo et al., 2006). From information security view, these characteristics may describe the organizational security practices and culture, security planning, security policy and risk mitigation strategies. After a thorough review of all the selected articles, several security and privacy issues discussed by the authors can be classified as organizational-related.

Organizational culture and awareness on the security and privacy issues brought upon by big data is an important factor to consider in safeguarding data from human-related breaches. Philips-Wren et.al. (Phillips-Wren et al., 2015) in their article revealed that addressing organizational culture in the context of big data is highly important. This importance is highlighted by the fact that "attitudes on ethics, privacy, and security can vary significantly across organizations". In another article that presents a paradigm shift in computational social science in big data era, best practices in safe handling of big data are said to come from the way organization provided encouragement and work structure to all of their employees instead of relying on individual's way of working with data. Thus, in order for organizations to derive the intended benefit of big data and to protect data from security breaches, organizations are required to make alterations and enhancement in terms of its business processes and applications in addition to making an incremental change in its business model (Buhl &

Heidemann, 2013). And, to avoid catastrophic consequences should there be a data breach, it is vital that organizations have the right protection mechanisms prepared – the consequences of wrongful treatment of customers or employees data must be made known throughout the whole organization (Lafuente, 2015). To make the changes in culture and awareness a successful effort, top management role is also important in promoting security culture and providing necessary support and security technology resources. Lack of top management support may deter the efforts made by IS security professionals in protecting and securing organizational data and systems from functioning at optimum level (Mbowe, Zlotnikova, Msanjila, & Oreku, 2014).

Another organizational-related issue derived from the review is organizational learning capacity and employees' competencies in the implementation of necessary big data protection mechanisms. As asserted by Chang et.al (Chang et al., 2014), implementation of protection required for a big data environment can be an expensive and challenging tasks. This process requires several necessary steps, such as designing data handling process, as well as identifying suitable training and procedures for employees. Other steps include periodic auditing of the protection mechanisms put in place and problem identification of security issues that may arise. Again, the authors stress for all employees to be aware of their responsibilities in the protection chain, and this demands for organization-wide effort. Organizational competencies and learning abilities will provide needed support in developing employees' competencies and skills in safeguarding big data environment (Chang et al., 2014). It is important for organizations to realize the need to relearn skills in managing the security and privacy of big data. Although some organizations may view the required skills as being similar to those needed for traditional business intelligence, there are some requirements which are unique to big data, e.g. strategies and policies required to identify and retain big data-ready workforce, managing security and privacy mechanisms that cater to the unique characteristics of big data,

defining storage parameters and methods for secure disposal of big data (Phillips-Wren et al., 2015).

Another issue is related to organizational development and use of big data - it is essential for organizations to ensure privacy principles are integrated into the development process. One author suggests that organizations with predefined privacy measures in development and use of big data, will garner the most desirable outcome and less number of consumer pushback (Goodendorf, 2013). Mennecke et.al. (Mennecke et al., 2014) supported this idea by stating that privacy principles should be built into business processes and information systems "as a default, rather than as an afterthought". System development that proactively address the need for security and privacy may potentially helped organizations should there be any privacy violation. In essence, getting big data security and privacy as an afterthought must be avoided at all cost. The importance for organizational recognition on the vital requirements in securing big data is undisputable, for it needs to be addressed and embedded in any development and use of big data components from the very beginning (Wang et al., 2015).

Several main issues can be derived from the review above, in relation to organizational-related security and privacy of big data. The first is organizational culture and awareness on the security and privacy requirements of big data. This may be translated to the need for organizational information security culture. With organization-wide and top management support, this culture may be cultivated and spread across the organization, hence minimising the risks associated to employee-linked security breaches. Another factor is organizational learning culture and competence. It is expected that organizational abilities to learn new protection procedures and new development processes that integrate security and privacy principles from the very start will lead to a more secure big data environment. These issues

may be studied further in order to explore the correlation between the issues and organizational intention to adopt big data.

5.6 Security and Privacy Issues in Environmental Context

Big data's security and privacy issues in environmental context are recognized in a number of articles. This context refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" (DePietro et al., 1990). Essentially, it suggests that there will be influences coming from the environment in which the organization operates whenever the organization is planning for new technology adoption. In a typical big data environment, the collections of data about individuals are often involved – achieved though organization's interaction with their consumers and through other business collaborations. Thus, whenever these sensitive data are collected and being used within and across organization, the issue of privacy and confidentiality will emerge (Hayashi, 2013). As such, organizations need to consider its external environment that may affect the use of sensitive data in its big data initiatives.

One environmental-related factor that often appeared in the reviewed articles is the issue of privacy and its associated rules and regulations. In protecting consumers' privacy and private data, many countries have introduced data protection act that aims to regulate the use of individual's personal identifiable information (PII) by organizations. For example, in an article that explores the main factors that affect the intention of individuals to grant their network operators to use their PII, Saenz et.al. (Saenz et al., 2013) indicated that governments "have attempted to protect individuals' privacy by enacting laws or directives, which must be followed by all sectors, including the highly regulated telecom industry".

While these enacted regulations are meant to protect the privacy of end consumers, it is fast becoming one of the challenges faced by organizations working with big data. Buhl and Heidelman (Buhl & Heidemann, 2013) in their editorial article agreed that numerous country-based privacy regulations and restrictions are "big data's most serious challenges". The authors also suggested that while present generation of consumers are no longer reserved when it comes to revealing their personal information while on the web, privacy regulations that are country-specific may seriously hinder big data initiatives and its corresponding business models. This impediment may also be attributed to a significant number of consumers who refuse to allow for a long-term storage of their private data (Buhl & Heidemann, 2013).

As the regulations that administers the use of personal data differs across countries, this will pose some pressure towards organizations wanting to leverage the potential of big data but at the same time having to abide to the legal provisions concerning the use of data (Kshetri, 2014). Privacy acts and regulations in the EU for instance, is generally considered as much stricter that the regulations in the US (foreign companies operating in the EU will have to abide to these regulations) (Martin, 2015).Consequently, an extensive big data governance program is needed in order for organizations to comply with society's ethical and governmental legal expectations (Chang, 2015; Jarke, 2013; Malik, 2013). Malik in his article asserts that security challenges of data sharing between applications as well as the compliance with "geographical trans-border data regulations" need to be addressed in any big data governance program. In addition, organizations are also expected to address the fundamentals of strong protection required for any personal, health and financial data (Malik, 2013). Inevitably, organizations will therefore need to deliver on these expectations without compromising their business goals, which can be a daunting task.

Security issues of outsourcing and the use of third-party tools is another environmental-related factor that can be found in the reviewed articles. In a big data environment, there may be a need for organizations to outsource some part of the tools and applications that support data storage, sharing and access (Jagadish et al., 2014). According to Wood (Wood, 2013), most organizations are still unable to build and maintain a full-fledged big data environment in-house. As a result of this incapacity, it creates dependence to, for example, service providers and other third-party tools vendors (Kshetri, 2014). The need to outsource, although critical to creating and capturing value of big data, will create the need for a further consideration on security and privacy. In one article that provides comprehensive overview of big data, Chen et.al. (Chen et al., 2014) reiterates the need to rely on professionals and tools in order to analyse huge datasets, which in turn will create further safety risks for the data. The authors then stress for a proper security measures to be put in place before the owner of big data delivers the datasets for processing and storage by third-party service providers. These measures are required as preventive mechanisms in protecting sensitive data (Chen et al., 2014).

Cloud computing services have consistently been linked to the operation of big data environment. Goodendorf (Goodendorf, 2013) in her article argued that the cloud is in fact needed for cost-effective implementation of big data. Even though this outsourcing practices are normally viewed as a way to transfer operational and adoption risks to the service provider, the truth is it does not eradicate the risks of data loss (Chang, 2015). Cloud storage for instance, may invite data security problems (e.g. requirements of data integrity checking) and it may also lead to privacy issues when the datasets are hosted in a server that is publicly accessible (Chen & Zhang, 2014). For a mitigation approach in ensuring security and privacy in the use of cloud services; Phillips-Wren et.al. (Phillips-Wren et al., 2015) suggested that organizations need to verify that a cloud service provider has an up-to-date security and privacy policies for data

sharing and inter/intra organizational collaboration. This approach is also supported by Goodendorf (Goodendorf, 2013), by stating that both cloud service provider and user organizations need to clearly define their responsibilities in regards to data privacy controls. The drawn contractual clauses must be more extensive than the standard general-security responsibilities (Goodendorf, 2013).

From the review above, it can be deduced that there are two highly possible environmental-related security and privacy concerns for organizations looking to embark on big data initiatives. The first factor is privacy related regulations while the second factor is organizational concern on outsourcing and use of third-party services. These two factors may possibly be the hindering factors for big data adoption due to lack of competency of some organizations in ensuring the security and privacy of big data that are externally hosted, and the difficulties in complying to unsurmountable privacy related regulations.

5.7 Conclusion

There are numerous contributions and publications in the big data area. Issues on security and privacy of big data particularly, have gathered great interest of academics and practitioners. However, these issues are still in its infancy in the IS domain. Based on the literature review conducted, security and privacy issues of big data are found to be mostly described within big data overview articles. Specific security and privacy articles otherwise, tackles the problems by introducing new framework, methods or processes in providing protection to big data components.

This study attempted to identify security and privacy issues from articles categorized under ‘overview’ and ‘security and privacy’ categories. Through the review, important security issues

and privacy concerns were classified under three major contexts: technological, organizational and environmental (taken from TOE framework – an organizational level technology adoption framework). The reason these three contexts were chosen as the classification framework is to provide future research with a foundation on the possible security determinants that may influence big data adoption by organizations. Based on the findings of the review, the main security and privacy issues that could possibly have an effect towards organizational intention to adopt big data were identified (refer to Fig. 5-1 below).

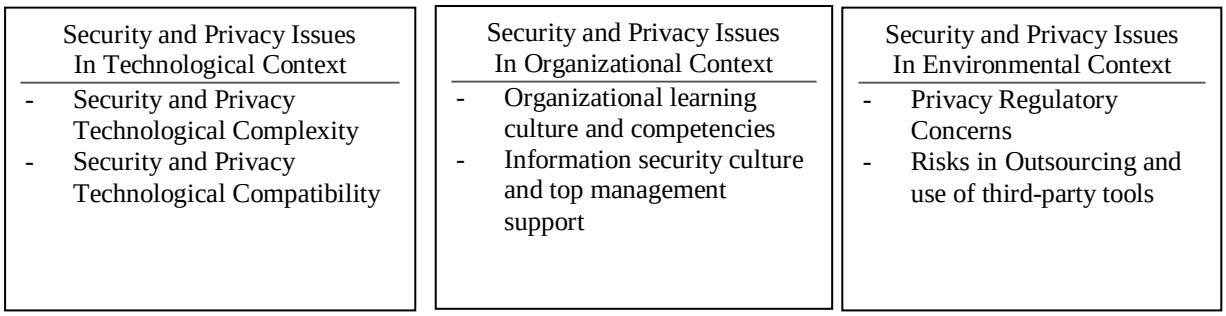


Figure 5-1: Identified Security and Privacy Issues for each Technological, Organizational and Environmental Context

From this preliminary literature review, it is evident that security and privacy issues of big data are not restricted to technological incapability, in fact, the problems and challenges may also arise from organizational culture as well as environmental facets. While these findings show the relevancy of looking at security and privacy issues of big data from different perspectives, and especially how these issues may play a role in encouraging/discouraging organizations' big data adoption, it is yet to be addressed empirically in IS publications. This fact opens up future research opportunities.

5.8 Limitations and Future Research

There are several limitations identified in this study. The major limitation is the use of only one keyword for every phases of literature search. Therefore, the resulting search returns may have

excluded some articles that discuss about big data in a different term such as ‘datafication’. Additional literature review should include other databases as well as this study only focuses on two citation indices – the SSCI and SCI. Furthermore, future research that aims to link the factors identified in this study with big data adoption, must also consider the inclusion of articles from technology adoption area.

The aim of a future research activity is to find appropriate conceptual framework that will be able to predict the causal relationship between the identified issues with big data adoption. With this framework, empirical investigation may be conducted to provide support for any developed hypotheses. Security and privacy issues have been quoted by some organizations as one of the hindering factors in big data adoption, thus it will be beneficial to seek for the actual issues that deter the adoption process. Organizational case studies will be one of the efficient methods to achieve clarification on how security and privacy issues may affect organizational intention to adopt new technology such as big data. Findings from this future research may be beneficial to practitioners by providing information on the factors that may hinder big data adoption as well as factors that can be leveraged to encourage adoption.

6. Sec-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption (Article 2)

6.1 Introduction

The amount of data being generated around the world at present is astounding and occurs at a rapid rate. This explosion of data gave birth to the term 'Big Data'. The term is often associated to three unique characteristics of data: *Volume, Variety*, and *Velocity* or more widely known as the 3Vs (Bansal et al., 2014; Gartner Inc, 2012) . Evolving trait of data being generated and stored has spurred the interest of organizations from various industries to adopt big data solutions (BDS) for solving specific business problems. However, as in any new technology adoption in organizations, BDS may also present security threats and challenges (Kshetri, 2014; Wood, 2013). Most threats are associated to the unique characteristics of big data, and the infrastructure that is required to support the size and scale of data collections (Demchenko et al., 2014; Mayer-Schönberger & Cukier, 2013). By having BDS, organizations will collect and process large amount of data and this include sensitive information of its customers and employees, intellectual property and trade secrets. When these data are stored centrally in a BD environment, it will attract cybercriminals who perceive the data as a valuable target for attacks (Tankard, 2012). This essentially shows that big data need to be properly protected with highest level of security mechanism.

In addition, due to the changing characteristics of data being handled by organizations, and the surge in information gathering, storing and reusing of personal data in business analysis process, big data has become "more dangerous than the Internet" (Mayer-Schönberger & Cukier, 2013). Thus, there should be a change in the way organizations manage and provide

control towards its data. The process of adopting BDS should not only be seen as a technology adoption in increasing organizational efficiency, but instead, a more holistic manner should be prescribed in making adoption decision.

Security aspects, besides from its technological and infrastructure need, should also be looked into from the organizational and environmental perspective. It has been agreed by security researchers that more research are needed to understand the interplay of organizational and environmental factors on information security issues (Da Veiga & Eloff, 2010; Singh, Gupta, & Ojha, 2014). In big data sense, making simple changes to existing rules and procedures may no longer be adequate in governing and control of data (Mayer-Schönberger & Cukier, 2013). With the huge amount of data being handled by organizations, sometimes up to petabytes of data, it should be a priority for organizations to include security-readiness assessment in the process of adopting new data-intensive technology such as BDS. At present, the scarcity of information on the security factors or concerns on BDS derived from empirical studies in organizations is regrettable because the information is important in supporting organizational decision in adopting BDS. While it can be seen that BDS is gaining momentum in its adoption by organization, and there is a growing concern on its security related factors; there is still a gap in research between the need to adopt it and the security factors that may affect the intention to adopt (Kshetri, 2014).

Summarizing on the above points, the intent of this research is to examine the security determinants by focusing on the influence that various security technologies, organizational security view and security related environmental factors have on BDS adoption. In addition, this research also aims to ascertain the degree of importance and role that information security plays in organization's decision or intention to adopt big data solution. This research in

progress paper starts with a literature review on BDS and research questions in section 6.2, followed by the proposed hypotheses and conceptual research framework in section 6.3. Section 6.4 presents the proposed research design and section 6.5 concludes the paper with expected contributions of the research.

6.2 Literature Review and Research Questions

This section provides a brief overview on BDS adoption, security concerns in BDS adoption, and theoretical foundation of the research. The research questions are presented at the end of this section.

6.2.1 Big Data Solutions Adoption

Various industries have traditionally worked with vast amount of data, for instance, the telecommunication and finance industries. At present, other industries have also started to look at the potential of exploiting complex data that originated from multiple sources, and existed in different format. BDS now begins to support analytic processes in "mobile services, retail, manufacturing, financial services, life sciences and physical sciences", to name a few (Bansal et al., 2014). Early adopters of big data solutions are aware of its potential to open up new business opportunities and provide better understanding of their business setting (Kwon et al., 2014).

The apparent expanding interest in big data in recent years is further confirmed by several studies conducted by market research firms. International Data Corporation (IDC)[1] for

[1] International Data Corporation is a market research company specializing in Information Technology.

example, states that the market for big data technology and services are expected to grow at 27%, compound annual rate, ultimately reaching to $32.4 billion in 2017 (IDC, 2013).

However, some organizations are still sceptical and thus holding back from venturing into big data domain. As asserted by Kwon et al. (2014), even though some organizations are already on the "forefront of big data analytics and thus are highly bullish" about its benefits and prospects, there are still a large segment of industry that have separate view over big data's purported values. A recent enterprise big data survey conducted by IDG shows several reasons cited by the respondents as the factors that inhibit the adoption of big data solution. Topping the list is budgetary factor, followed by limited skilled employees that are able to manage and analyse big data, as well as security issues (IDG Enterprise, 2014). The above findings demonstrate that organizations are aware of big data approaches and solutions, and these organizations are showing a keen interest to invest in them. This increasing interest in big data and its related concerns provides a venue for this research to study the factors that will positively and negatively affect its adoption.

6.2.2 Security Concerns for Big Data Solutions

Security and privacy factors have consistently appeared as one of the challenges in BDS adoption (Big Data Working Group, 2013). Kshetri (2014) points that the existing non-big data security solution may not have the capability to properly address the security issues that comes from the "scale, speed, variety and complexity" of big data. Thus, it is important for organizations seeking to embark on big data initiatives to recognize the unique characteristics of big data that undoubtedly will lead to new security and privacy threats. When making decisions to adopt BDS, compatibility between an organization's current security technology and the intended BDS should be among the factors to consider. The first characteristic of big

data - *Volume*, refers to the huge size of data set collected and created from a diverse range of sources. High data volume would present a danger in security, for example, it may attract the attention of cybercriminals and could lead to security breach (Kshetri, 2014). One of the key challenges is to provide security technologies and solution that are able to scale to the large size of data sets and distributed nature of big data (Demchenko et al., 2014).

The second general characteristic of big data, *Velocity*, which describes the speed in which data are being created and the speed of how it should be analysed and acted upon; may also pose some security threats. Many organizations are currently generating high frequency of data and this may create difficulties in maintaining the security of data. Among the security issues that may be associated with the rapid frequency of data creation is the lack of technological security capabilities to have a secure storage for large amount of data particularly during peak data traffic (Kshetri, 2014). For instance, during peak data traffic, it will be much harder to detect security breaches and provide appropriate response to attacks – and the absence of a secure storage for huge volume of data will only amplify this problem.

The third characteristic, *Variety*, also poses significant security issues and challenges. Variety refers to the various data sources and types of data being collected and stored in any big data environment. Thus far, organizations are familiar in the handling of the security measures in protecting structured data, but with the combination of unstructured data, the experience in ensuring security may be lacking (Kshetri, 2014). In a report of a survey on the governance of unstructured data sponsored by Varonis Systems (2008), it is noted that technology solutions in securing unstructured data are still in growing phase and governance issues are still not addressed. When data are collected from variety of sources, one key security issue that may arise is the issue of input validation and untrusted input sources. It will be difficult to identify

malicious data sources, and, the need to filter malicious input from the diverse range of data sources will also be a daunting process.

Besides from security issues that require technological solution, organizational security practices and culture should also be among the focus factors in making decision to adopt BDS. Organizational dimension denotes characteristics that represent an organization, such as company strategies, culture, structure and policies (Teo et al., 2006) . From information security view, these characteristics may describe the organizational security practices and culture, security planning, security policy and risk mitigation strategies. In addition, a big data environment often involves the collection of data about individuals and the data originates not only from within the organization, but are also mined from external sources (Göb, 2014).

Thus, whenever these sensitive data are collected and being used within and across organization, the issue of privacy and confidentiality will emerge (Hayashi, 2013). As such, organizations need to consider its external environment that may affect the use of sensitive data in its big data initiatives. Among the environmental issues that require the attention of organizations adopting big data are privacy regulatory issues as well as outsourcing and use of third party tools (Kshetri, 2014).

As many non-scholarly outlets have reported findings that security is one of the reasons that hinders the adoption of BDS, it is thus timely and important to extend the results to academic research in order to identify the security factors that have actual impact on BDS adoption.

6.2.3 Theoretical Foundation

Technological-Organizational-Environmental (TOE) Framework

TOE framework was first introduced by DePietro, Wiarda and Fleischer in a book chapter titled *The Context for Change: Organization, Technology and Environment* (DePietro et al., 1990). This general framework in innovation studies, describes three contexts; *technological, organizational* and *environmental*, that may influence the process of technological innovation adoption at firm level. The technological context refers to both internal and external technologies relevant to the firm. Technology in this context may denote both equipment and processes (DePietro et al., 1990). Essentially, it is believed that the fit between the existing technology setting in a firm, and the intended technology innovation will be one of the determinants in the decision to adopt technology innovation.

The second context is organizational context. It refers to multiple characteristics that represent a firm in general and can be in the form of organizational strategies, culture, structure as well as policies (Teo et al., 2006). These formal and informal processes and structures in turn may have an effect in the adoption of technological innovation within organizations.

The environmental context refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" (DePietro et al., 1990). This context fundamentally implies that in order for organizations to adopt new innovation or technology, there will be influences coming from the environment in which the organization operates. The external factors may include organization's clients, suppliers, its market competitors, government regulations and other related external pressure

and forces. For the purpose of this research, all constructs under each of the three contexts will be aligned on security concerns to suit the central aim of this research (Sec-TOE).

6.2.4 Research Questions

The number of organizations that are using BDS is growing, thus making security factors associated with securing data capture and storage infrastructure a higher concern (Bansal et al., 2014; Rubinstein, 2012). Therefore, this research attempts to provide answers for the following research questions:

1. How do technology factors in security, organizational security view, and security-related environmental factors encourage/discourage organizations' big data solution adoption?

The identified security factors in each technological, organizational and environmental context will be examined for its correlation with BDS adoption through hypothesis testing.

2. How does information security shape organizational decision to adopt big data solutions?

This part of the study will be based on the outcome of the first hypothesis testing. A case study will be conducted in order to ascertain the role that information security plays in adoption of BDS, and to see whether there are any changes in the way information security is perceived when making decisions to adopt BDS (level of InfoSec importance in BDS adoption as compared to other technological adoption).

Besides from providing answers for the two questions above, this research also aims to provide recommendations on security factors and measures that may be leveraged by organizations in BDS adoption. Hence, the following two questions are formulated:

3. How are changes in security measures being made by organizations adopting big data solutions?
4. What recommendations on security management aspects can be introduced for organizations adopting big data solutions?

A conceptual security-based BDS adoption framework will be developed and recommendations on security management aspects in BDS adoption will be introduced based on the findings and outcome of the hypothesis testing and case study.

The hypotheses and framework that will be presented in the next section are formulated to provide answers to the first research question. The rest of the research questions will be addressed during the second qualitative phase of the research.

6.3 Research Hypotheses and Framework

This section presents the research hypotheses and framework that is structured according to TOE framework. The dependent variable for this study is adoption of BDS - which refers to a collection of technologies and framework that provides a "platform to integrate, manage, and apply sophisticated computational processing to big data" (Davenport 2014, p. 120). BDS adoption refers to organizations' intention and decision to select, install and implement BDS in the future, or otherwise, for organizations that have already deployed BDS, the decision to continue using it.

6.3.1 Technology Factors in Security

Perceived Complexity

In the context of this research, perceived complexity describes the technological complexity of big data – as presented by its characteristics of volume, velocity and variety, which then leads to perceived complexity in ensuring its security. In a big data environment, the need for security technologies and controls that is flexible enough to effectively address changing requirements may affect the perceived complexity as viewed by organizations. Hence, higher level of perceived complexity will produce higher level of uncertainty in relation to successful adoption and implementation of new technology (Tornatzky & Klein, 1982). Thus, it is posited that:

> H1: Perceived complexity in ensuring the security of big data negatively affects the adoption of big data solutions.

Perceived Compatibility

The term 'compatibility' is defined as the perceived fit of an organization's current security technology and control with the security requirements of BDS. In previous technology adoption research, compatibility factor has frequently been found to exert an influence on adoption of new technology (Borgman et al., 2013; Kwon & Zmud, 1987). Compatibility of security technologies and controls in securing various enterprise systems, hardware and software has improved over the last decade, but, with big data, new security concern and issues arises which may not be addressable by present security technologies (Hashem et al., 2014). Hence, when an organization perceived compatibility between their current security technology and control

with the security requirements of a BDS, the chances to adopt the solutions will be higher. Based on the above facts, the following hypothesis is proposed:

H2: Perceived compatibility of present security technology with security requirements of big data solution positively affects the adoption of big data solutions

6.3.2 Organizational Factors in Security

Top Management Support

Top management support refers to the level of commitment and involvement of organizations' top management in IS security for BDS adoption. It is known that the amount data being created and handled in a big data environment are huge; therefore, larger datasets have to be protected. In doing so, it is important to have the support of the top management. Several studies have demonstrated that organizational security culture and security policy enforcement will be higher following an increase in top management support (Hu, Dinev, Hart, & Cooke, 2012; Knapp, Marshall, Rainer, & Morrow, 2004).

Top management may manifest their support for security practices by being actively involved in the security risk assessment of new technology, formulation of IS security and observing organizational IS security practices (Kankanhalli, Teo, Tan, & Wei, 2003). Based on the above argument, it is posited that:

H3: Top management support for IS security positively affect the adoption of big data solutions.

Information Security Culture

Information security culture denotes "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997). While security breach and risks have long been the concern of organizations, it is anticipated that with the introduction of big data, security risks will increase (Kshetri, 2014). One of the risks to information security within organizations is human behaviour, and this has been proven by various prior studies (Pahnila et al., 2007; Workman, Bommer, & Straub, 2008).

Realizing the problem of human behaviour towards information security, many researchers have proposed for embedment of information security culture within organizations. Information security culture is believed to diminish risks to information assets, by exerting influence to employees in protecting organizational information (Schlienger, 2003; Van Niekerk & Von Solms, 2010). Thus, the following hypothesis is proposed:

> H4: Embedded information security culture within organization positively affects the adoption of big data solutions.

Organizational Learning Culture

Organizational learning culture refers to the learning characteristics and orientation of an organization especially in the process of complex technology adoption. Previous literatures have provided support for the notion that organizations with strong learning characteristics have the ability to adeptly learn any new technologies, have embedded processes to scan for risks, identify opportunities and provide solutions (March, 1991; Nambisan & Wang, 1999). In safeguarding a big data environment, organizations may need to learn on the security risks

associated with the characteristics of big data. Thus, these new security requirements signify the need to learn will arise. In relation to this, organizations that exhibit a positive and high level of learning culture will be able to decrease the knowledge barriers that deter the adoption of new technology (Fichman & Kemerer, 1997). As such, the following hypothesis is proposed:

H5: Strong organizational learning culture positively affects the adoption of big data solutions.

6.3.3 Environmental Factors in Security

Security and Privacy Regulatory Concerns

Security and privacy regulatory concerns refer to organizational concerns in ensuring compliance to security and data privacy regulations. For organizations that are embarking on big data initiatives, it will be a challenge to ensure compliance to traditional data protection regulation, specifically due to the characteristics of data being generated, stored and reused. Traditional data protection regulations were mostly created and introduced based on the premise of structured data, which is simpler to manage and assess to ensure its appropriate use (Cumbley & Church, 2013).

Whereas, ensuring compliance to data privacy act is far more complicated with unstructured data that essentially form the bulk of big data. Most organizations would want to make certain that they fully comply with regulations, but, the amount of unstructured data that they have to work with in a big data environment, may make it hard for them to do so (Kim, Trimi, & Chung, 2014).

Thus, it is posited that:

> H6: Security and privacy regulatory concern negatively affect the adoption of big data solutions.

Risks of Outsourcing

Risks of outsourcing refers to the associated security and privacy risks that may result from organizational decision to outsource their big data initiative, or the use of third-party tools in their BDS. As BDS is relatively new, most organizations are still without the capability to build and maintain an in-house big data environment (Wood, 2013). Thus, this creates a need for organizations to resort to outsourcing practices – for its whole big data environment or part of it (Jagadish et al., 2014).

Organizational dependence to service providers and third-party tool vendors will come with some security associated risks. This is shown by various studies that found security risks are among the main concern of organizations planning to outsource their IT technologies and infrastructure (Nassimbeni, Sartor, & Dus, 2012; Trustwave, 2013). Thus, this research posits that:

> H7: Risks of outsourcing negatively affect organization's decision to adopt big data solutions.

Based on the hypotheses presented above, Figure 6-1 illustrates the conceptual research framework.

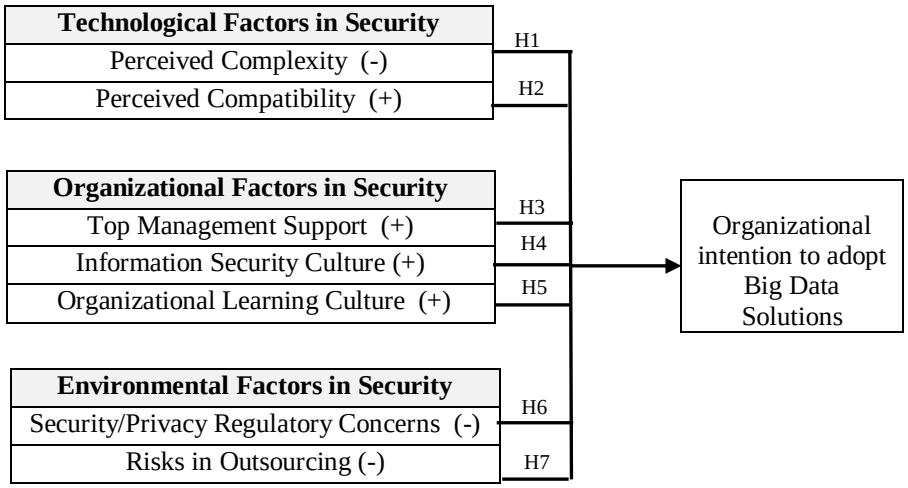


Figure 6-1: Sec-TOE Framework – Security Determinants in BDS Adoption

6.4 Research Design

Based on the characteristics of this research, a sequential explanatory mixed method design is found to be the appropriate method to be employed. Sequential explanatory mixed method approach is a two-phase mixed method approach that aims to have qualitative data that will assist in clarifying initial quantitative result (Creswell & Clark, 2011). The first phase of this research is a quantitative study formulated to test a conceptual framework of big data solution adoption through the evaluation of security factors that may affect its adoption in organizations.

Hypotheses testing will be done through the process of construct operationalization, instrument development, sample identification, survey distribution, data collection, and results analysis. The strategy of inquiry for this first phase is questionnaire survey. The target recipients of the survey are organizations' employees that are knowledgeable about their organization's technology adoption practices and/or those who are responsible for security practices in the organization.

The sampling frame for this research will be public listed companies in both New Zealand and Malaysia. These two countries were selected to represent two categories of big data maturity ranks (IDC's categorisation of Asia Pacific's countries based on their ranking in BD maturity) (IDC, 2015); New Zealand for *Leaders* and Malaysia for *Starters*. Stratified random sampling will be used to identify the final pool of samples. The stratums will be divided into type of industries that will have the highest likelihood of having big data; e.g. financial, telecommunication, health and retail. The unit of analysis for this research is organization. Statistical analysis to support testing of the proposed hypotheses will be performed using statistical tools. Correlation coefficients will be determined for each independent variable in order to evaluate its relative strength as a factor affecting the dependent variable – BDS adoption. Statistical tool will also be used to perform factor, correlation, and regression analysis.

The second phase of the research is a qualitative study that aims to explain in depth and follow up on the outcome and data generated by the quantitative study. The qualitative research methodology that is chosen for the research is a single case study method. The case study organization will only be identified after the quantitative study in order to ensure a link between the first phase quantitative study and the second phase qualitative study. Data collection techniques that will be used for the case study are interviews and document observation. The interview sessions aim to elicit interviewee's interpretation of their organizational security and big data solution adoption experiences and their understanding of them.

The coding process will be applied to all transcribed interviews to facilitate the identification of matching concepts or themes from the different interviews. Initial coding categories and a coding schema will be derived from theoretical considerations obtained from a review of

relevant literature and the proposed conceptual framework. After the completion of both phases, a sequential data analysis procedure will be conducted in order to derive overall findings and interpretation. The purpose of this sequential analysis is to seek answers on how the qualitative data may help in explaining the results gained from the quantitative study (Creswell & Clark, 2011).

6.5 Conclusion

While security concerns have been cited by organizations as one of the barriers in adopting BDS, there has been no empirical evidence on the security factors that have actual impact on its adoption. Thus, the main objective of this research is to investigate the security factors that may affect the adoption of BDS. With the sequential explanatory mixed-method approach that will be employed for this research, it is hoped that the researcher will be able to produce an elaborate answers and expand the outcome of one method (quantitative) with another method (qualitative). The final outcome of this research is expected to have both practical and theoretical contribution. This research aims to provide a conceptual model of security factors that may affect the adoption of BDS, as well as providing recommendations on the security factors that may hinder adoption and the factors that may be leveraged to increase chances of adoption. This research also aims to contribute to the body of knowledge on technology adoption, BDS, and information security. The mixed-method approach will also be of significance in a qualitative-dominated InfoSec management research in IS field.

7. Adoption of Big Data Solutions: A Study on its Security Determinants using Sec-TOE Framework (Article 3)

7.1 Introduction

Big data is a term that emerged in the last few years and its associated technologies are now relevant across industries and economic sectors. This phenomenon is in part due to the proliferation of digital data; in addition to the vast amount of data being produced by data-intensive organizations. While the technologies that supported big data has been one of the most talked about technology trends in recent years, there is still no concrete definition to the term big data itself. Hence, the term is normally described by practitioners and researchers according to its traits. The common associated traits are: "volume –large amount of data", "variety – different types of data collected", and "velocity – speed of data transfer and creation" (Bansal et al., 2014) . However, one common view can be derived; big data consist of huge data sets, with various data types and sources produced and transferred at great speed. These characteristics create a difficulty in managing and processing data using traditional data processing techniques or saving it in any traditional structured relational database management systems.

To fully harness the potential of big data, organizations are starting to seek for technologies and solutions that have the ability to process and analyse these various sources of data and data types (Davenport & Dyche, 2013). Technologies and solutions for big data such as Hadoop systems are now available for selection and deployment by organizations. Looking at the benefits of deploying big data solutions (BDS) specifically in terms of its ability to store, accumulate and combine large datasets, organizations are now well aware of how big data will

enable rigorous data processing, thus making deep analyses of data more accessible (Wielki, 2015). Pioneering business and organizations have started to exploit the benefits of big data in creating value for their operation in order to remain competitive. These early adopters of BDS are aware of its potential to open up new business opportunities and provide better understanding of their business setting.

Even though some organizations are already on the "forefront of big data analytics and thus are highly bullish" about its benefits and prospects, there are still a large segment of industries that have separate view over big data's purported values (Kwon et al., 2014). A recent Enterprise Big Data survey conducted by IDG Enterprise shows several issues cited by the respondents as the factors that inhibit the adoption of BDS. Among others, security and privacy issues were found as one of the hindering factors (IDG Enterprise, 2014). In other surveys conducted by market research companies and technology providers, security and privacy issues have also consistently been named as one of the top hurdles or challenges in organizations' big data efforts (Gartner Inc, 2014; Sans Institute, 2015). This finding demonstrates that business and IT executives believe BDS may posed new security threats and challenges, as commonly encountered during new technology adoption in organizations (Kshetri, 2014). Accordingly, having BDS installed does not only require effective management of storage and retrieval of data, as it also encompass the need to address the various privacy issues and security-related threats. The threats unique to BDS may be contributed by the characteristics of big data itself; the variety, velocity and volume of data. These unique characteristics magnifies the challenges for managing big data security as opposed to managing traditional data environment (Nasser & Tariq, 2015). Else, the security features of BDS such as the open-source Hadoop is also lacking in its initial design. It was evidently not designed with security features in mind, as it was solely intended to handle large data storage and fast processing. Regardless of Hadoop's

security weaknesses, it is presently receiving wide integration with organizations' existing IT infrastructure and consequently introduces security vulnerabilities (MIT Technology Review, 2015).

While there is a growing number of publications that report on privacy and security issues in relation to big data, the number of empirical findings on its adoption by organizations and its associated security factors that may influence the intention to adopt is still scarce (Ahmad Salleh, Janczewski, & Beltran, 2015; Kshetri, 2014). Although it is safe to conclude that Big Data solutions are gaining momentum in its acceptance and importance across industries, there are still security issues and challenges in relation to big data, which dampens the adoption by certain businesses and organizations. Can the deterring factors be attributed to diverse perception on the complexity of securing big data environment, a lack of top management support in acknowledging the importance of information security for new adopted technology, or the need to comply with security and privacy related regulations? These issues create research opportunities to comprehend the security related factors pertinent to big data adoption in organizations.

It is therefore the aim of this study to look into adoption factors, specifically from security aspects that may encourage or discourage the adoption of BDS. Theoretically, this study applies the TOE framework (Technology-Organization- Environment) by DePietro, Wiarda and Fleischer (1990) to answer the following research question:

How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption among adopter and non-adopter organizations?

This paper presents the preliminary descriptive findings of the study. The remainder of this paper is organized as follows: section 7.2 describes the conceptual research framework, followed by the research methodology in section 7.3. Section 7.4 presents the results from descriptive analysis and discussion. This paper ends with a section that concludes the findings, limitations of this study and details of planned future works.

7.2 Conceptual Research Framework

For the purpose of this study, an organizational level technology adoption framework – the TOE framework (DePietro et al., 1990), is adapted to align with the security factors that we believe influences BDS adoption in organizations (Sec-TOE framework). Figure 7-1 illustrates the conceptual framework for this study.

7.2.1 Sec-TOE Framework

The TOE framework is a general framework in innovation studies that describes three contexts that may influence the process of technological innovation adoption and implementation at organizational level. The three contexts are: technological, organizational and environmental (DePietro et al., 1990). To address the research question of this study, the TOE framework is adopted and the constructs under each of the three contexts are adapted to align with security related factors, hence the name Sec-TOE (Ahmad Salleh et al., 2015). The technological context refers to internal and external technologies relevant to an organization. As asserted by Tornatzky and Fleischer (1990), the fit between the existing technology setting in an organization and the intended technology innovation will be the determinant in the decision to adopt technology innovation. Thus, the main emphasis is on how the adoption process can be

influenced by technology characteristics themselves (Chau & Tam, 1997). Two technological constructs were used in this study; *perceived complexity,* and *perceived compatibility.*

The TOE framework's second context is organizational. This context comprises of multiple characteristics that represent an organization in general. The characteristics may include organizational strategies, culture, structure as well as policies (Teo et al., 2006). These characteristics may either be a constrain or facilitating factor in the adoption of new technology by organizations (Oliveira & Martins, 2011). Organizational context for this study comprises of three constructs; *top management support, information security culture,* and *organizational learning culture*. The third context – environmental, refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" (DePietro et al., 1990). Primarily, this context implies that there will be influences from the environment in which an organization operates when dealing with technology adoption. For this context, the constructs used were *security/privacy regulatory concerns* and *risks in outsourcing*.

7.2.1.1 Organizational Intention to Adopt BDS

The dependent variable for this study is organizational intention to adopt BDS. In this context, BDS refers to a collection of technologies and framework that provides a "platform to integrate, manage, and apply sophisticated computational processing to big data" (Davenport, 2014, p. 120). BDS adoption signifies organizational intention and decision to select, install and implement BDS.

7.2.1.2 Perceived Complexity

Perceived complexity in the context of this study is defined as the perceived degree of difficulty and understanding in providing security mechanisms for BDS. Higher (perceived) complexity is normally associated with higher level of uncertainty in relation to successful adoption of new technology (Grover, 1993). In a big data environment, the need for security technologies and controls that is flexible enough to effectively address changing requirements may affect the perceived complexity as viewed by organizations. Thus, we postulate that a higher perceived complexity in ensuring the security of BDS will negatively affects organization's intention to adopt BDS.

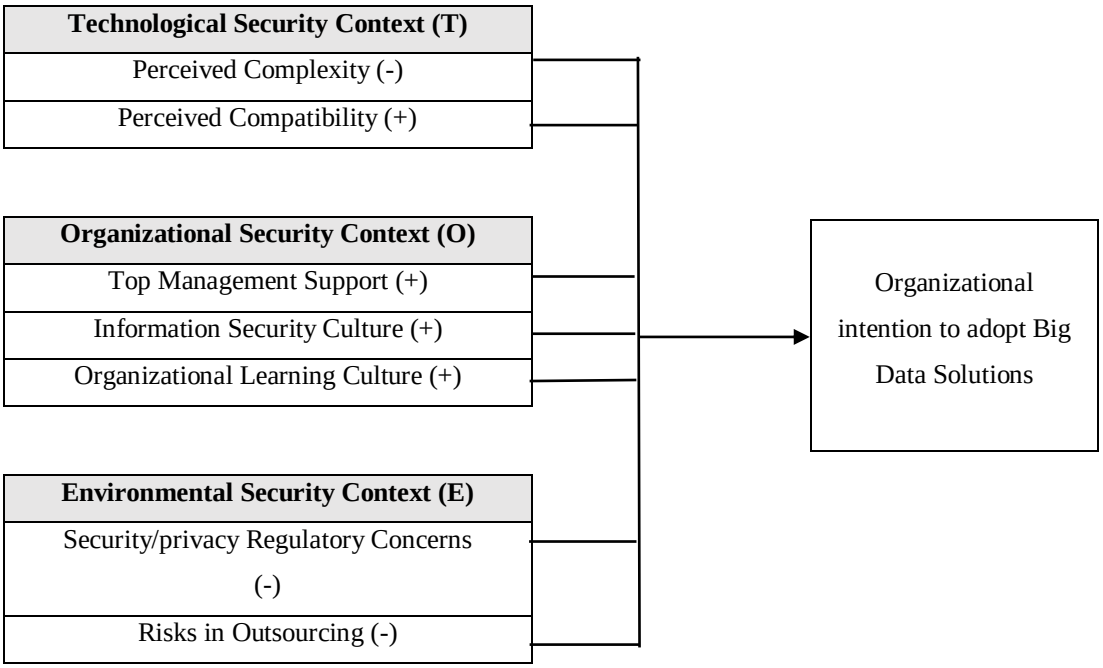


Figure 7-1: Sec-TOE Framework – Security Determinants in BDS Adoption

7.2.1.3 Perceived Compatibility

The term 'compatibility' refers to "the degree to which an innovation is perceived as being consistent with the existing value, past experiences, and needs of receivers" (Rogers, 2003). In

this study, perceived compatibility reflects the degree to which an organization's current security technology and control mechanisms are perceived as fit with the security requirements of BDS. As compatibility factor has consistently been found to exert influence in new technology adoption (Borgman et al., 2013), this study posits that perceived compatibility of organization's present security technology and mechanisms with security requirements of BDS positively affects organization's intention to adopt BDS.

7.2.1.4 Top Management Support

This study defines top management support as the level of support and commitment given by organizations' top management towards IS security requirement and mechanisms involved in BDS adoption. With the support of top management, financial and technical resources are highly likely to be made available specifically for IS security. Additionally, organizational security awareness and policy enforcement will also be more effective (Hu et al., 2012), thus creating a stable environment for new technology adoption such as BDS. Thus, it is expected that top management support for IS security will positively affect organization's intention to adopt BDS.

7.2.1.5 Information Security Culture

Information security culture denotes "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997). Within any big data environment, the handling of huge amount of data that comes from different sources and at a great speed will intensify organizational risks in being a victim of information security abuse. Human behaviour has consistently been cited as one the risks to information security abuse within organizations (Pahnila et al., 2007). Embedded information security culture may

exert influence on employees to diminish human behaviour risks to information assets by protecting organizational information (Van Niekerk & Von Solms, 2010). For this reason, this study hypothesizes that embedded information security culture within organizations positively affects organization's intention to adopt of BDS.

7.2.1.6 Organizational Learning Culture

Learning characteristics and orientation of an organization is important during complex technology adoption process. By having a strong learning characteristics, an organization will have the ability to adeptly learn new technologies, scan for risks, identify opportunities and provide solutions (Nambisan & Wang, 1999). BDS for example, may require security personnel to identify new risks associated to it, and learn on new mechanisms for its protection. Considering this, organizations that exhibit a positive learning culture will decrease knowledge barriers that may deter BDS adoption. Hence, a positive organizational learning culture is anticipated to positively affect organization's intention to adopt BDS.

7.2.1.7 Security and Privacy Regulatory Concerns

Security and privacy regulatory concerns in this study refers to the degree of concern in ensuring compliance to security and data privacy regulations in relation to BDS adoption. Traditionally, data protection regulations is simpler to manage and adhere to since it were mostly created based on the foundation of structured data (Cumbley & Church, 2013). Big data otherwise, consist of mostly unstructured data, thus ensuring compliance to privacy regulations is far more complicated. This is turn, may result in significant reduction of interest in big data exploitation by organizations. For this, it is hypothesized that security and privacy regulatory concern negatively affects organization's intention to adopt BDS.

7.2.1.8 Risks in Outsourcing

This study defines risks in outsourcing as perceived degree of security and privacy risks associated to outsourcing (outsource BDS or the use of third-party tools). Organizations interested in embarking on big data initiatives may have to start with outsourcing the whole big data environment or part of it. As BDS is relatively new, most organizations are still without the capability to build and maintain an in-house big data environment (Wood, 2013). The need to outsource may introduce security and privacy associated risks, a dependency towards vendors and organizations will need to relinquish some control of their information assets over to vendors. Thus, this study posits that risks in outsourcing negatively affect organization's intention to adopt BDS.

7.3 Methodology

Data for this study were collected using an anonymous online questionnaire survey administered in New Zealand. The questionnaire comprises of three sections. The first section consists of items relating to respondents' organizational background which includes a question on the level of BDS adoption in respondents' organization. The second section assesses organization's perception on technological, organizational and environmental security factors using a five-point Likert scale ranging from "Strongly Disagree (1)" to "Strongly Agree (5)". The questionnaire ends with one question that asks the respondents to rate their level of concern on BDS security from a scale of 1 to 10 (1=Low, 10=High) and an open-ended question on organization's main security and privacy concern on BDS based on any principles of the CIA triad. Survey items for each constructs were mainly identified from prior studies and adapted to the context of the study.

The survey items were then reviewed by 2 academics in information systems field, 1 practicing information security professional and 1 doctoral student to ensure content clarity of the overall questionnaire. The survey was administered to New Zealand Information Security Forum (NZISF), a special interest group which members have a common interest in information security. Purposive sampling was used and deemed suitable for this preliminary study as it was intended to test the instrument and derive an estimation of results before the actual survey is administered. In total, 25 responses from 70 selected members were recorded, yielding a response rate of 35.7 percent. Given the small sample size, it does not allow for a robust parametric/inferential statistical analysis. Thus, this study primarily looked at descriptive analysis to explore the collected data.

7.4 Results and Discussion

Descriptive statistics of the respondents and their organizations are presented in Table 7-1. Most of the respondents were from organizations that have more than 2000 employees and are handling 1 to 100 terabytes of data per month. Out of the 25 valid responses, 15 (60%) are classified as adopters and 10 (40%) non-adopters.

The results also revealed that adopters were mostly medium to large sized organizations and are managing 500GB to above 1TB of data per month. This finding shows that adopter organizations fulfilled the initial requirement of BDS implementation: having the *volume* of data to work with. Descriptive statistics and internal consistencies for the two constructs under *Technology* context are presented in Table 7-2. The Cronbach Alpha for *perceived complexity* and *perceived compatibility* are 0.812 and 0.864 respectively, showing a satisfactory internal consistency of the measurement items.

Table 7-1: Descriptive Statistics of Respondents and Their Organizations (N=25)

Category	Frequency	Percentage (%)
Job Position		
• Chief Information Officer (CIO) / IT Director	1	4%
• IS/IT Management/Staff	13	52%
• Info. Security Management/Staff	8	32%
• Others	3	12%
Industry		
• Consumer Goods	3	12%
• Education	3	12%
• Energy and Natural Resources	1	4%
• Financial Services	2	8%
• Government/Public Sector	1	4%
• Healthcare/Pharmaceuticals	1	4%
• IT and Technology	9	36%
• Telecommunications	2	8%
• Others	3	12%
Number of Employees		
• Less than 50	1	4%
• 51-100	2	8%
• 101-500	2	8%
• 501-1000	6	24%
• 1001-2000	4	8%
• More than 2000	10	40%
Amount of Data Handled Per Month		
• Above 100 TB	2	8%
• 1 to 100 TB	7	28%
• 500 GB to 1 TB	4	16%
• 100 GB to 500 GB	2	8%
• Below 100 GB	2	8%
• Not aware of the amount	8	32%
BDS Adoption Level		
• Adopted	15	60%
• Do not adopt	10	40%

This study posits that a higher *perceived complexity* in ensuring security of BDS negatively affect the intention to adopt BDS. Findings show that the mean for perceived complexity is indeed higher for organizations classified as non-adopters (3.80) than the mean for adopters (3.22). The highest level of agreement for the non-adopters went to the item that states integrating security requirements of BDS in their current work practices will be very difficult (4.10). One measurement item – CX2, has high standard deviations for both adopters and non-adopters (>=1). This may imply high variance of perception on the complexity of skills required to secure BDS. Although the adopters' mean score (3.00) indicate uncertainty on the

complexity of skills required, the high standard deviation shows that some respondents agreed on the skills complexity and some who did not. Different level of knowledge, experience and skills of the respondents in information security and complex technology in general, may be the factors that lead to this varied perception.

Table 7-2: Descriptive Statistics for Perceived Complexity and Perceived Compatibility

Measurement Items (Perceived Complexity)		**Adopters (N=15)**		**Non- Adopters (N=10)**	
		Mean	Std. Dev.	Mean	Std. Dev.
CX1	Establishing information security mechanisms for BDS is difficult and complex	3.40	.910	3.70	.675
CX2	The skills required to secure BDS are too complex for our employees	3.00	1.0	3.60	1.075
CX3	Integrating security requirements of BDS in our current work practices will be very difficult	3.27	.704	4.10	.568
	Cronbach's Alpha = 0.812 **Total**	3.22	.452	3.80	.447
(Perceived Compatibility)					
CP1	The changes introduced by BDS is compatible with the organization's existing information security practices	3.40	.828	3.00	.444
CP2	Security requirements of BDS is compatible with the organization's existing information security infrastructure	3.40	.828	2.80	.844
CP3	Development of info security mechanisms for BDS is compatible with the organization's existing experiences with similar systems.	3.47	.743	2.90	.989
	Cronbach's Alpha = 0.864 **Total**	3.42	.375	2.90	. 390

As for *perceived compatibility*, the assumption is that a perceived compatibility of an organization's present security practices and mechanisms with the security requirements of BDS will positively affect the intention to adopt it. Looking at the mean score for both adopters (3.42) and non-adopters (2.90), this assumption seems valid. Whilst the mean score is indeed higher for the adopters, a score of 3.42 is closer to 3.0 (uncertain scale), demonstrating that some adopters tended to be uncertain of the compatibility of their organization's present security practices and mechanisms with those of BDS requirement. Being a relatively new technology, potential security compatibility issues introduced by BDS might not be fully

encountered and understood by adopters. Else, compatibility issues might not be considered as significantly different from the adopters' normal operating challenges (Borgman et al., 2013).

Table 7-3 presents the means, standard deviations and internal consistencies of all three constructs under *Organizational* context. The reliability and internal consistencies of the measurement items for the three constructs were shown to be satisfactory based on its Cronbach Alpha value of above 0.7. From the table, it can be seen that the means of *top management support* for non-adopters clearly falls behind the means of the adopters (2.88 vs 3.84). The findings seem to show an agreement towards the assumption that top management support for IS security will positively affect the intention to adopt BDS. This suggests that commitment and support from the top management will indeed create a conducive environment for adoption of new technology innovation (Borgman et al., 2013). Support given by top management through effective communication and tolerance towards newly introduced risks will help in providing the necessary security mechanisms required by less mature technology such as BDS.

The mean scores for all items measuring *information security culture* were relatively high for adopters. These high averages suggest the existence of information security culture in adopters' organizations. As can be seen in the table, there's a difference in the total means for adopters (4.01) and non-adopters (3.53). With this, support is given to this study's initial proposition that embedded information security culture within organization will have a positive effect towards intention to adopt BDS. Embedded information security culture as part of organizational traits will help to instill security awareness among employees and thus helping the organization to avoid security risks associated to human behavior (Lim, Ahmad, & Maynard, 2010). Consequently, this culture will lead to an improved security level for the whole organization, making it more secure to host data intensive technologies such as the BDS.

Table 7-3: Descriptive Statistics for Top Management Support, Information Security Culture and Organizational Learning Culture

Measurement Items (Top Management Support)		Adopters (N=15)		Non- Adopters (N=10)	
		Mean	Std. Dev.	Mean	Std. Dev.
TS1	Top management supports the adoption of BDS	3.87	.743	2.80	.400
TS2	Top management accepts possible risks which may result from adopting BDS	3.87	.640	2.80	.622
TS3	Top management takes information security issues into account when planning to adopt BDS	3.87	.743	3.20	1.289
TS4	Top management allocates budget and manpower for information security functions	3.73	.799	2.70	.678
TS5	Top management effectively communicated its support for information security goals associated to BDS adoption	3.87	.640	2.90	.322
	Cronbach's Alpha = 0.919 **Total**	3.84	.267	2.88	.509
	(Information Security Culture)				
SC1	Information security is a key norm shared by the employees of this organization	4.00	.535	3.60	.966
SC2	Employees of this organization value the importance of information security	4.07	.594	4.00	.816
SC3	A culture exists in this organization that promotes good information security practices	3.80	.676	3.40	1.075
SC4	Information security has traditionally been considered an important organizational value	3.87	.834	3.10	1.101
SC5	Practicing good security measures is the accepted way of doing business in this organization	4.20	.561	4.00	.471
SC6	This organization has dedicated efforts to create an information security- focused workforce	4.13	.640	3.10	1.287
	Cronbach's Alpha = 0.839 **Total**	4.01	.440	3.53	.667
	(Organizational Learning Culture)				
LC1	There is an agreement that the organization's security function's ability to learn is the key to information security effectiveness	4.07	.458	3.80	.422
LC2	The basic values of the security function in this organization include learning as key to improvement	4.13	.516	3.80	.789
LC3	The sense around the organization is that employee learning is an investment, not an expense	3.73	.799	3.20	1.229
LC4	Learning is seen as a key commodity necessary to guarantee organizational survival	4.00	.845	3.70	.949
LC5	The collective wisdom in this organization is that once we quit learning, we endanger our future	4.07	.799	3.40	.843
LC6	This organization encourages its employees to pursue security certifications/accreditations	4.33	.488	3.30	.675
	Cronbach's Alpha = 0.740 **Total**	4.06	.490	3.53	.683

Similar results were shown for *organizational learning culture*. Comparing the means for adopters and non-adopters, the means for adopters (4.06) is found to be considerably higher than those of non-adopters (3.53). Almost all of the measured items scored a mean of above 4.00 hence suggesting a high level of agreement by the adopters to the importance of organizational learning culture on information security effectiveness. By having a positive learning environment, security function of any organization will have the ability to learn on new security mechanisms, identify potential risks brought by new technology, and will have a more positive outlook on the complexity of newly adopted technology such as the BDS (Fichman & Kemerer, 1997).

The means, standard deviations and internal consistencies of the two variables for *Environmental* context are shown in Table 7-4. Test of internal consistencies for both variables resulted in Cronbach Alpha value of 0.794 for *security and privacy regulatory concern*, and 0.852 for *risks in outsourcing*. The Cronbach Alpha values demonstrated the reliability of measurement items for both variables. As depicted in the table – the mean score for *security and privacy regulatory concerns* shows a small difference between adopters (3.75) and non-adopters (3.87). This study hypothesized that higher concern for security and privacy related regulation associated to the use of big data will negatively affect the intention to adopt BDS, but the relatively small difference in the mean scores found it to be inconclusive. Thus, based solely on the mean scores, it can be said that both adopters and non-adopters are highly concern on the need to comply with security and privacy regulations. One explanation for this is, organizations that have traditionally worked with high volume of data would have been trained to familiarize themselves with data security and to always be aware of requirements for regulatory compliance. This proposition may especially be true for organizations operating in any highly regulated industries; e.g. finance, healthcare.

Table 7-4: Descriptive Statistics for Regulatory Concerns and Risks in Outsourcing

Measurement Items (Security and Privacy Regulatory Concerns)		Adopters (N=15)		Non- Adopters (N=10)	
		Mean	Std. Dev.	Mean	Std. Dev.
RC1	Adherence to security standards and privacy regulations is a challenge with the collection, storage, analysis and reuse of big data	3.93	.704	4.00	1.054
RC2	It is harder to assess the compliance of all personal data collected by BDS with the requirements of data protection law	3.73	.884	3.90	.876
RC3	With the use of BDS, there is a concern of legal implications due to non-compliance to security standards and privacy regulations	3.60	.910	3.70	.823
	Cronbach's Alpha = 0.794 **Total**	3.75	.414	3.87	.521
	(Risks in Outsourcing)				
OR1	The need to outsource BDS creates concerns on data security and privacy	3.47	.915	4.20	.632
OR2	The need to outsource BDS creates vulnerability in access control of the organization's information asset	3.80	.862	3.90	.994
OR3	The need to outsource BDS creates risks through excessive dependency towards vendor	3.20	1.014	3.70	1.160
OR4	The need to outsource BDS complicates the process of implementing corporate policy in protecting individual privacy and data security	3.40	.910	4.00	.667
	Cronbach's Alpha = 0.852 **Total**	3.47	.448	3.95	.498

The means score for *risks in outsourcing* shows a clear difference between adopters and non-adopters (3.47 and 3.95 respectively). While both means are above the uncertain scale (>3.0), the mean is higher and closer to 4.00 (agree scale) for the non-adopters. These results indicate that the non-adopters were more concern about the risks associated with outsourcing practices. The highest mean out of the four measurement items went to OR1, where the non-adopters agreed that the need to outsource BDS creates concerns on data security and privacy. Both adopters and non-adopters seem to have high variances in their answers for OR3, which states that the need to outsource BDS creates risks through excessive dependency towards vendor (std. dev. >1.0). Organizations with prior involvement in outsourcing for example, may have assembled experiences and skills in outsourcing practices. Thus, working with their

outsourcing partners were not seen as inviting the risks of excessive dependency – hence possible disagreement of some organizations on item OR3.

7.5 Conclusion, Limitation and Future Work

This study is a preliminary investigation into BDS adoption from the context of information security. TOE framework is adopted as the conceptual research framework and adapted to measure information security related factors (Sec-TOE) that may influence organizational intention to adopt BDS. Theoretically, this study contributes to the existing technology adoption framework by conceptualizing security related factors as predictors to BDS adoption by organizations. Besides the usual constructs used in other studies that was based on TOE framework, this study introduces two new constructs under the *Organizational* context; *information security culture* and *organizational learning culture*.

Based on descriptive analysis conducted, it is revealed that organizations classified as adopters have a relatively high agreement towards the following adoption determinants; perceived compatibility, top management support, information security culture and organizational learning culture (all four are predicted to have positive effect on intention to adopt BDS). Whilst, the non-adopters were shown to be negatively affected by the following two factors; 1) perceived complexity and 2) risks in outsourcing. Security and privacy regulatory concern was one determinant factor found to be inconclusive. The result shows that both adopters and non-adopters have a very similar level of concern on the need to comply with security and data protection regulations.

While the results of this study demonstrate the path to which the Sec-TOE framework is heading in relation to influencing BDS adoption, more robust data are needed to provide stronger empirical evidence for all the hypotheses. The limitations of this study include a small number of respondents, sampling method used that may not capture the actual view of organizations and incapability to conduct hypothesis testing. As this study is a part of future studies planned, the main objective is to have an initial view on the reliability of the framework. For the next phase, the plan is to conduct a survey with a wider population. The target population are public listed companies in New Zealand and Malaysia. This quantitative study will then be complemented by a single case study aimed to derive further support on how information security may affect the intention to adopt data-intensive technology such as BDS. The case study is also aimed to elicit any other security determinants in BDS adoption that may have been left out in the initial Sec-TOE framework presented in this study.

8. An Implementation of Sec-TOE Framework: Identifying Security Determinants of Big Data Solutions Adoption (Article 4)

8.1 Introduction

In today's data driven era, big data has become one of the most talked about terminology across businesses and industries. Due to increasing awareness on its potentials, big data concept and its associated technologies has also garnered the interest of academia and has now appeared in numerous academic research and discussions. In principle, big data refers to massive amount of varied-format digital data. It is prompted via proliferation of digital data and vast data creation by data-intensive organizations. Even though big data has been consistently discussed in both academic and non-academic publications, the exact definition of the term is still ambiguous. Thus, the term is typically defined according to several characteristics unique to big data. Three main characteristics regularly associated to big data are; 1) Volume 2) Variety and, 3) Velocity or widely known as the 3Vs. *Volume* describes very large amount data, *variety* refers to different types and sources of data while *velocity* refers to the speed of data creation and processing (Chen & Zhang, 2014). Besides the 3V's, many researchers have included other 'Vs' to describe the characteristic of big data, for instance *Veracity* – verifiable data and its trustworthiness, and *Value* – added-value resulting from processed data (Clarke, 2016). These unique characteristics differentiate big data from other types of datasets used in traditionally known data processing techniques.

At present, more organizations are looking to exploit big data to reap its benefits and to create value for their operation in order to remain competitive. To harness big data's full potential, these organizations have started to seek for solutions and technologies specifically tailored for

big data processing. Open source software framework Hadoop for example, has gained widespread recognition as one solution for big data's distributed storage and processing (Chang et al., 2014). Other technology giants have also developed and offered their own brand of big data solutions (BDS) to organizations. With the availability and deployment of these solutions, organizations will be better equipped to perform rigorous data processing on their large datasets, and deep analyses of data are made more accessible (Shim et al., 2015). Organizations that are considered as pioneers in big data deployment have now moved from experimenting stage to profiting from big data. These early adopters of BDS gained from its awareness of big data's potential in creating new business opportunities and providing their organization better understanding of their business needs.

Although some organizations have become leaders in the use of big data and thus are optimistic in terms of its potentials and benefits, a large segment of businesses are still having doubts and reservations towards big data's publicized values (Kwon et al., 2014). Recent surveys conducted by marketing research and technology consulting companies have shown that there are several factors that hinders organizational BDS adoption. For example, in a survey conducted by IDG Enterprise in 2015 (Big Data and Analytics Survey), nine factors were found to have an impact during organizational evaluation of solution offerings made by data and analytics vendor (IDG Enterprise, 2015). Among the nine factors, ability to meet security requirements of BDS became the second prioritized factor for enterprise organizations (the first priority went to issues in integrating BDS into existing infrastructure). Security and privacy issues of big data have also been consistently cited as one of the top inhibiting adoption factors in other similar surveys (Gartner Inc, 2014; Sans Institute, 2015).

Findings of these surveys establishes that there are concerns among organizations on security and privacy threats and challenges posed by big data. Newly encountered security threats and challenges are common occurrence in any technology adoption process, but in the case of big data, its extent of reach to diverse functions in organizations may introduce far greater exposure to security and privacy risks (Demchenko et al., 2014). Organizations that chose to have BDS installed not only have to ensure effective management of creation, storage and retrieval of data, but also need to deal with various privacy issues and security threats. The unique characteristics of big data; mainly the 3Vs, are among the contributors to security and privacy threats associated with the use of BDS. Each of these characteristics present its own security and privacy concerns that necessitates a reliable security solutions and mechanisms in ensuring the confidentiality, integrity and availability of data. Moreover, these characteristics amplifies the challenges of managing security requirements of big data in contrary to managing traditional data environment (Nasser & Tariq, 2015).

Threats to security and privacy in BDS also existed due to lack of security features in early development of the solutions. Hadoop for instance, was not designed with default security features in place even though it is meant to provide a platform for distributed storage and processing of large datasets. While there are weaknesses in Hadoop's security, this framework is still being widely integrated with existing organizational infrastructure, creating vulnerabilities (MIT Technology Review, 2015). Despite these vulnerabilities, there are still security professionals who could not understand the reasons for treating security as a big issue when they have their first encounter with big data environments (Lane, 2014) . This demonstrates that the degree of difficulty and impact of big data related security issues are yet to be realized by security professionals. The presence of threats to security and privacy in fact, justifies the need for organization-wide awareness and understanding on the difference between

security requirements of a traditional database environment with those required by a big data environment.

The number of academic and non-academic publications on big data's security and privacy related issues are constantly growing. Whilst the number of publication is large, empirical findings that reported on the specific security and privacy related issues that is of concern to organizations in BDS adoption are still scarce or rarely discussed in publications (Kshetri, 2014). Although it is safe to conclude that BDS are gaining wider acceptance across industries, still there are security issues and challenges in relation to big data which may deter organizations from adopting BDS. Various security related factors may have an impact on organizations' decision in BDS adoption such as diverse perceptions on level of complexity in securing big data environment, compatibility of organizations' current security infrastructure with the requirements of BDS, organizational information security culture, and risks in outsourcing BDS, among others. These issues in turn, create research opportunities in identifying and understanding organizational point of view in security and privacy factors significant in BDS adoption.

Hence, this research aims to study the security related factors that may encourage or discourage the adoption of BDS in organizations. Theoretical framework applied in this first of a two-part study is TOE framework (Technological-Organizational-Environment) (DePietro et al., 1990), a technology adoption framework which is adapted to suit the needs of this research. Key research question that motivated this research is: *How do technology factors in security, organizational security view and security-related environmental factors encourage/discourage organizations' big data solution adoption?* To better understand these issues, a conceptual model for security determinants in BDS adoption based on TOE framework was developed.

This paper presents the result of a survey conducted among public listed organizations in New Zealand and Malaysia. The following sections in this paper are organized as follows: section 8.2 provides a brief discussion on the theoretical perspectives of the study and presents the conceptual model and hypotheses. The research methodology is then presented in section 8.3, followed by data analyses and results in section 8.4, and discussion in section 8.5. This paper ends with a brief summary of the findings, statements of research limitations and planned future work.

8.2 Theoretical Perspectives

This study focuses on security-related determinants in organizational intention to adopt BDS. Results of several big data surveys have established security and privacy related issues as among the inhibitors in organizational intention to adopt big data. In order to understand which security related issues that may become the determinants in BDS adoption, these issues were analyzed based on one theoretical foundation: the TOE framework.

8.2.1 TOE Framework and Security Determinants in BDS Adoption

A theoretical model on security determinants in BDS adoption needs to take into account diverse security-related factors that may affect organizational intention to adopt BDS. Besides the common technological issues, security-related factors may also be contributed by organizational and environmental circumstances of an organization. After reviewing literatures, the TOE framework (DePietro et al., 1990) was found to be useful as a starting point in looking at the diverse security determinants in BDS adoption. The TOE framework identifies three contexts that influences the process by which an organization adopts, implements, and

uses technological innovations. The three contexts are: technological, organizational and environmental (DePietro et al., 1990).

The first context; technological, describes internal and external existing technologies in use as well as new technologies which are relevant to an organization. Tornatzky and Fleischer (1990) asserts that compatibility between an organization's present technology settings with the intended technology innovation plays a determining role during organizational decision-making process for new technology adoption. Technology in this context may include current practices, equipment and processes (Oliveira & Martins, 2011). Hence, the key emphasis of this context is on how these technology characteristics can influence the process of technology adoption. For this study, considering the security-related factors that are of interest, two technological constructs were included in the conceptual model; 1) perceived complexity and 2) perceived compatibility.

The second context in a TOE framework - organizational, includes multiple characteristics and resources that generally represent an organization. Among the characteristics that falls under this context are; organizational strategies, culture, structure and policies (Teo et al., 2006). It is believed that adoption of innovative technologies by organizations may either be facilitated or constrained by the above characteristics (Oliveira & Martins, 2011) . This study selected three constructs for the security-related organizational context; 1) top management support, 2) information security culture, and 3) organizational learning culture. The TOE framework's environmental context relates to the area "in which an organization conducts its business, for example, its industry, competitors, access to resources supplied by others, and dealing with the government" (DePietro et al., 1990). For this context, it mainly implies that the environment in which an organization operates may influence organizational intention and decisions during

technology adoption. For this study, two constructs deemed relevant to environmental security-related considerations were chosen; 1) security/privacy regulatory concerns, and 2) risks in outsourcing.

Based on published literature review on the use of TOE framework in studying technological innovation (e.g. Oliveira and Martin 2011), it can be concluded that TOE framework provides consistent empirical support in multiple IS domain. By adopting TOE framework as theoretical foundation, this study will add to the framework's pool of empirical findings of IS related research – specifically in information security. All constructs listed above and the conceptual research model will be explained further in the next section.

8.2.2 Conceptual Model and Hypotheses

Using the TOE framework, a conceptual model was developed to assess security determinants in organizational adoption of BDS. The model distinguishes between three building blocks determining the intention to adopt BDS: technological context, organizational context, and environmental context. All constructs included in the model are security-related constructs, hence this model is aptly named Sec-TOE. Each construct represent either security-related constraint or opportunity for the adoption of BDS. The conceptual model is presented in Figure 8-1. Descriptions on the key constructs of the model and its associated hypotheses are presented next.

The endogenous construct (dependant variable) in this study is organizational *intention to adopt BDS*. To describe BDS, a definition provided by Davenport (2014, p.120) is used; BDS refers to a collection of technologies and framework that provides a "platform to integrate,

manage, and apply sophisticated computational processing to big data". Whereas, BDS adoption intention implies the decision made by organizations to select, install and implement BDS.

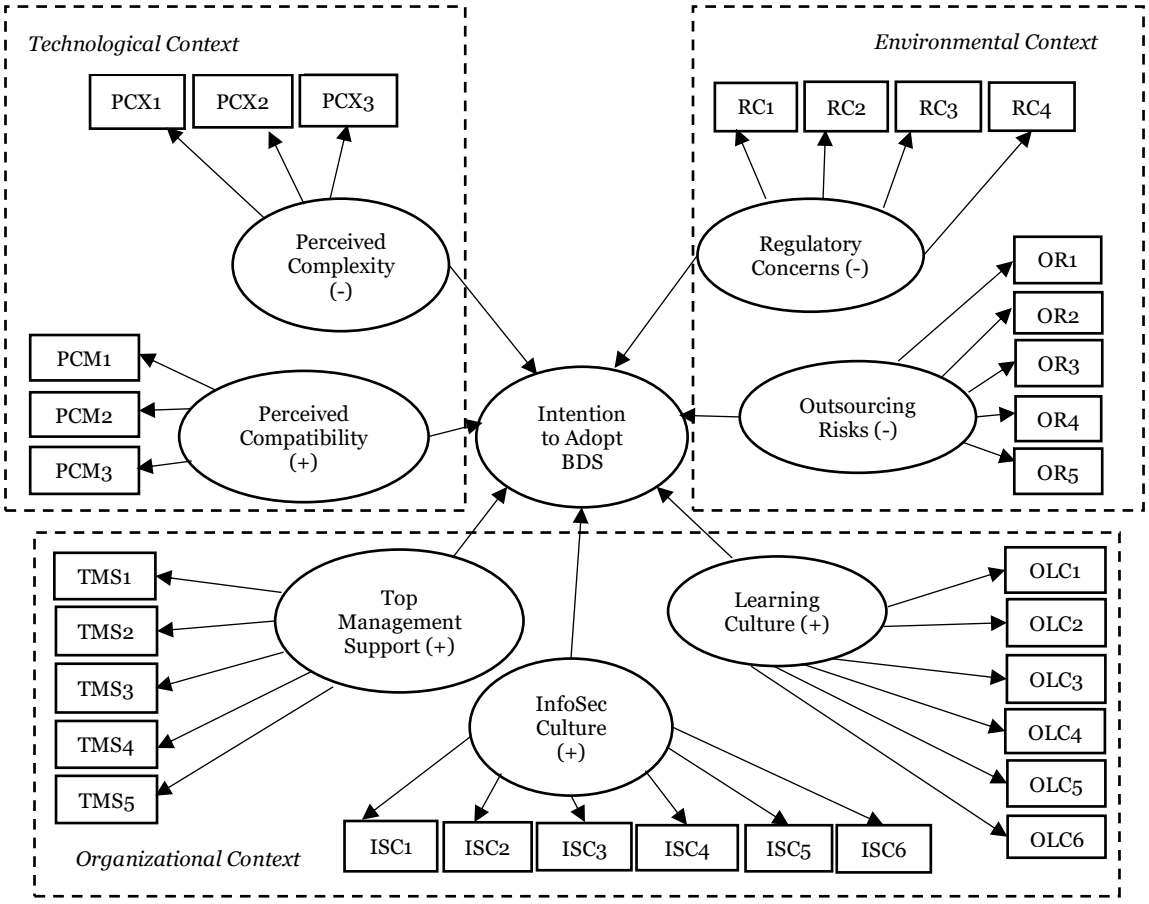


Figure 8-1: Conceptual Model of Security Determinants in BDS Adoption (Sec-TOE)

Perceived Complexity: Complexity can be described as "the degree to which an innovation is perceived as …. difficult to understand and use" (Rogers, 2003). In the context of this study, perceived complexity refers to the degree (perceived) of difficulty and understanding in providing security mechanisms for BDS. According to Grover (1993), higher level of uncertainty related to successful implementation of innovative technology are normally contributed by higher (perceived) complexity. In any big data environment, the "volume" characteristic of BD, is expected to pose challenges to existing security technologies and solutions. Due to the sheer volume of data collected and created in a big data environment, new

and improved security tools and mechanisms are needed to provide effective protection towards data (Chen & Zhang, 2014). The need for security technologies and controls that is flexible enough to effectively address changing security requirements may affect organizational view of its perceived complexity. Hence, it is posited that:

H1: Higher perceived complexity in ensuring the security of BDS negatively affects organization's intention to adopt BDS.

Perceived Compatibility: Compatibility reflects "the degree to which an innovation is perceived as being consistent with the existing value, past experiences, and needs of receivers" (Rogers, 2003). This factor has been frequently cited as having positive correlation with innovative technology adoption in past research. For this study, perceived compatibility is defined as the degree (perceived) to which an organization's current security technology and control mechanisms are compatible with security requirements of BDS. In an article by Adrian Lane (2014), the author stated that many security professionals found no reason to be alarmed with big data environment when they first encounter it. Although at present, while most organizations are familiar with security mechanisms required to protect structured data, but with BD and inclusion of unstructured data, deploying existing security mechanisms may present compatibility issues when coupled with organization lack of experience in handling BDS (Kshetri, 2014). Since compatibility factor has consistently been found to exert influence in new technology adoption (Borgman et al., 2013), this study posits that:

H2: Perceived compatibility of organization's present security technology and mechanisms with security requirements of BDS positively affects organization's intention to adopt BDS.

Top Management Support: Previous studies have found top management support as one critical element in creating supportive environment and providing essential resources in adoption of innovative technologies (Borgman et al., 2013; Wang, Wang, & Yang, 2010). This study denotes this factor as the level of support and commitment given by organization's top management towards IS security requirement and mechanisms involved in BDS adoption. Stronger top management support led organizations to engage in more preventive efforts, and may also encourage positive user attitude towards the use of IS (Kankanhalli et al., 2003). Studies have also found that low level of top management support leads to an organizational culture less tolerant of good security practices (Knapp, Marshall, Rainer, & Ford, 2006). Whilst, assigning acceptable risk levels for information assets and its relative worth to an organization during implementation of innovative technology such as BDS is best done by the top/senior management. Top management is in the best position to make such decision to ensure adequate supply of resources and effective policy enforcement (Hu et al., 2012; Young, 2010); stabilizing organizational environment for innovative technology adoption such as BDS. Based on the above argument, the following hypothesis is proposed:

H3: Top management support for IS security positively affects organization's intention to adopt BDS.

Information Security Culture: Information Security Culture can be defined as "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997). The term also refers to organizational efforts in relation to information security practices (Da Veiga & Eloff, 2010; Da Veiga, Martins, & Eloff, 2007). Among the risks faced by data-intensive organizations are security breaches contributed by human behaviour. In fact, human behaviour has regularly been identified as a risk that leads to

information security abuse within organizations (Pahnila et al., 2007). To mitigate this issue, one of the suggestions made by past researchers is to embed information security culture as part of organizational culture (Lim et al., 2010). Organizations with embedded information security culture is believed to have the ability to reduce risks associated with human behaviour. This can be done by exerting influence towards its employees in protecting organizational information assets (Van Niekerk & Von Solms, 2010). A big data environment will need to be protected at various levels of its creation and use, thus, having high level of awareness on information security (culture) is essential for organizations looking to adopt BDS. For this reason, this study hypothesizes:

H4: Embedded information security culture within organizations positively affects organization's intention to adopt of BDS.

Organizational Learning Culture: Organizational learning can be described as the ability or processes in an organization that enables the acquisition, access and revision of organizational memory, which in turn leads to organizational actions (Robey, Ross, & Boudreau, 2000). With strong learning characteristics, organizations will be able to learn new technologies, scan for risks, identify opportunities and provide solutions (Nambisan & Wang, 1999). Organizations planning to adopt innovative technology such as BDS may encounter some implementation barriers if there is lack of learning capacity among its employees. For instance, new security requirements of BDS will require security personnel in organizations to undergo learning process to bridge the gap between what they currently know and what is required by BDS. Without continuous learning ability, the effectiveness of the organization's present security mechanisms may not be sufficient in addressing new risks introduced by BDS. A positive organizational learning culture plays a key role in shaping innovative technology adoption.

Issues encountered during adoption and implementation can be explained and resolved; thus reducing associated knowledge barriers (Lin, 2008). Hence, the following is hypothesized:

H5: Positive organizational learning culture positively affects organization's intention to adopt BDS.

Security and Privacy Regulatory Concerns: This study defines security and privacy regulatory concerns as the level of concern organizations have towards the requirement to comply to security and privacy regulations. Legislation environment may have two sided effects towards innovation; it can either be beneficial or detrimental (Baker, 2011). It will be beneficial, for example, when governments introduced regulations that provide tax incentives for organizations adopting a certain technology. Adversely, it can be detrimental when governments introduced constraining regulations such as data security and privacy act. In the case of BDS, ensuring compliance to privacy regulations is far more complicated as it involves a mixture of both structured and unstructured data (Cumbley & Church, 2013). Few organizations will have the ability to fulfil each aspects of data security and privacy act for every single bit of data that they generate and process. Previously, data protection act is simpler to manage and comply with since it was mostly developed based on structured data. Excessive legislation and privacy restriction has a higher likeliness to dampen organizations' interest to participate in BD initiatives. Thus, it is posited that:

H6: Security and privacy regulatory concern negatively affects organization's intention to adopt BDS.

Risks in Outsourcing: IT outsourcing has been a major trend among organizations for several reasons. Among the reasons are; cost cutting, to improve efficiency, launching new business ventures, and to focus their resources towards their core competencies (Khidzir, Mohamed, & Arshad, 2010; Tafti, 2005). In this study, risks in outsourcing is defined as perceived degree of security and privacy risks associated to outsourcing (outsource BDS or the use of third-party tools). Risks refers to any undesirable events that may occur as the outcome of outsourcing practices. For relatively recent technology such as BDS, organizations may be required to outsource their whole BDS initiative or part of it due to the incapability of organizations to develop or maintain its own BDS environment (Wood, 2013). Without careful considerations of various security and privacy risks associated to IT outsourcing, organizations may become vulnerable to significant losses in terms of data privacy, data security and financial losses among others (Tafti, 2005). Ideally, organizations need to be more aware of the security mechanisms provided by service providers before signing a contract with them. In sum, besides the anticipated benefits of outsourcing, it may also present some security and privacy risks, and excessive dependency towards service providers. Organizations may also need to surrender some control of their information assets over to service providers. This study therefore hypothesizes the following:

H7: Risks in outsourcing negatively affects organization's intention to adopt BDS.

8.3 Research Methodology

Survey method was used to test the conceptual model in Figure 8-1 and the associated hypotheses. The survey method was chosen due to its ability to form generalizability, replicability and to produce results with statistical power. A questionnaire was designed based

on a comprehensive literature review and after a successful preliminary study, the final survey was administered in two countries.

8.3.1 The Constructs

All constructs in the model were developed based on comprehensive literature review in addition to some inputs from information security experts. Even though TOE framework has been adapted in numerous IT adoption studies, none of the constructs used in these studies were based on information security view. Since the constructs for each technological, organizational and environmental context in this study were based on information security issues, most of the indicator items used to measure the constructs were adapted from findings/statements made in previous organizational information security related studies.

Perceived Complexity: This construct was operationalized as a reflective construct that measures the degree of perceived complexity and understanding in providing security mechanisms for BDS. 3 items were used as indicators of the construct (PCX1, PCX2 and PCX3). To gauge the perceived degree of complexity from respondents, a 5-point scale was used ranging from 1=Strongly Disagree to 5=Strongly Agree.

Perceived Compatibility: Measuring the degree of perceived compatibility of organizations' current security infrastructure with the security requirements of BDS, this construct consist of 3 indicator items (PCM1, PCM2 and PCM3). 5-point scale with 1 reflecting the least agreement to compatibility and 5 to indicate full agreement to compatibility, was used as measurement scale of this reflective construct.

Top Management Support: This reflective construct aims to measure organizational top management support towards IS security requirements and mechanisms involved in BDS adoption. A 5-point scale was used to assess the extent of top management support in respondents' organization through 5 indicator items (TMS1 to TMS5). The indicator items include statements that seek respondents' level of agreement to top management support for BDS adoption, risks in adoption, IS security issues, allocation of budget and manpower to security function as well as effective communication.

Information Security Culture: There are 6 indicator items used to measure this construct (ISC1 to ISC6). Operationalized as a reflective construct, a 5-point scale was used to determine if there's a presence of information security culture within an organization. The indicator items seek for respondents' level of agreement to their organization's norm, values and practices involving information security and its mechanisms.

Organizational Learning Culture: Aimed to measure the existence of learning culture within an organization (specifically within the organization's security function), this construct was also operationalized as reflective. It has 6 indicator items (OLC1 to OLC6) intended to assess the respondents' level of agreement towards their organization's security function's learning ability and, whether learning is valued as key to information security effectiveness and improvement. A 5-point scale was used to measure this construct.

Regulatory Concerns: Operationalized as reflective, this construct consists of 4 indicator items (RC1 to RC4) which are measured using a 5-point scale. All items were developed to measure organizational concerns on the impact of privacy related regulations towards the adoption and use of big data.

Outsourcing Risks: This construct measures the perceived degree of security and privacy risks associated to outsourcing BDS or the use of third-party tools. 5 indicator items (OR1 to OR5) were used to measure this reflective construct based on 5-point scale. Respondents were asked to state their level of agreement on the risks and vulnerabilities in outsourcing BDS and its impact towards their organization's information assets, data security/privacy and access control.

Intention to Adopt BDS: To measure this endogenous reflective construct, respondents are required to indicate whether 1) their organization is contemplating BDS adoption and 2) their organization has adopted or likely to adopt BDS within a year. These measurement on adoption intention is based on Teo et. al. (2003). Both indicator items were anchored on a 5-point scale (1=Strongly Disagree to 5=Strongly Agree).

8.3.2 The Preliminary Survey

A preliminary survey was conducted after a conceptual validation process of the constructs and its multiple indicators. For this study, an anonymous online questionnaire was developed and administered to New Zealand Information Security Forum (NZISF) – a special interest group in New Zealand which members have a common interest in information security. This preliminary survey was done to test the instrument and derive an estimation of results before the actual survey is administered. Results received from the preliminary survey were analyzed and some amendments to the questionnaire were made based on suggestions and comments given by respondents. Descriptive analysis conducted during this stage reveals that BDS adopters' display a higher level of agreement towards the following positive BDS adoption security-related determinants; *perceived compatibility, top management support, information*

security culture, and *organizational learning culture*. For non-adopting organizations, the intention to adopt BDS is shown to be negatively affected by *perceived complexity*, and *risks in outsourcing*.

8.3.3 The Survey

A package containing a cover letter, an invitation note, participant information sheet (detailing the research background, objectives and procedure), consent form, a prepaid reply envelope and a copy of the questionnaire was sent to CEO/CIO of each identified public listed organizations in New Zealand and Malaysia. The questionnaire was also made available online, using an online survey tool – *Qualtrics*. In total, 148 survey packages were sent to New Zealand organizations and 205 to Malaysia (finance, consumer and trading services organizations). Public listed organizations were chosen as the sampling frame for this study as it includes majority of organizations that have a higher likeliness in generating big data. Contact information were gathered from NZX company research database and Bursa Malaysia. CEO/CIO of each organization was informed to select one respondent that has the best knowledge of their organization's technology adoption practices and/or information security practices/policies. Definition and description of BDS were included as part of the survey instrument to improve understanding and validity of responses.

Of the 353 questionnaires sent out, 52 responses from New Zealand organizations and 65 from Malaysia were received through both mail and the online survey tool. The responses were checked for consistency and 14 invalid responses were dropped. This screening process resulted in a final dataset of 103 responses; 44 from New Zealand and 59 from Malaysia (29.1% response rate). The final dataset was then examined for any potential biases that may resulted from the two-country data collection process (organization's size, number of responses,

respondent's BDS adoption status). No significant biases were found among the two countries. Further, common method bias was also examined using Harman's one factor test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). The result from this test shows that the dataset does not suffer from common method bias issues as the variance explained by a single factor is less than 50% (21.065%). In sum, these tests reveal that the dataset does not display any significant biases contributed by the survey methodology.

8.4 Data Analyses and Results

During analyses stage, the conceptual model was tested using the combined final dataset from both countries. Analyses were done in three steps; 1) preliminary analysis to identify any biasness and to derive descriptive statistics, 2) assessment of the measurement model and, 3) assessment of the structural model.

8.4.1 Preliminary analysis

Before the data collected from both countries were combined, the data were screened and analyzed for any anomalies. Monotones were deleted and missing value analysis was then performed. Little's MCAR test revealed that the missing value occurred at random, thus Expectation Maximization (EM) technique was used to treat and replace the missing values. Next, normality check using Shapiro-Wilk test returned a p value of less than the chosen alpha level of 0.05 ($p<0.01$ for data from both New Zealand and Malaysia). This value rejected the normality hypothesis of the test. To compare differences between the countries, non-parametric Mann-Whitney U test was chosen due to the endogenous variable being ordinal and not normally distributed. The asymptotic significance level derived from the test is 0.459 ($p>0.05$), hence it can be concluded that the data does not provide statistically significant evidence of

difference between New Zealand and Malaysia in its median *Intention to Adopt BDS* (the endogenous variable). Based on this result, the data collected from both countries were than pooled for use in further analyses of the conceptual model.

Out of the 103 final responses received, 47 organizations were BDS non-adopters and 56 were adopters. Most of respondents are the IS or IT management/staffs of their organizations (48), 23 responses were from information security management/staffs, 16 from head of business unit or department, 8 CIOs and another 8 from other categories of job functions. The three largest industries represented by the responding organizations were consumer goods, retail and financial services with 22, 14 and 13 responses respectively. 5 of the responses came from organizations that processes above 100 terabytes of data per month, 36 organizations with 1 to 100 terabytes of data per month, 36 that works with less than 1 terabyte and 26 respondents were not aware of the amount/size of data.

The profile of the responding organizations is provided in Table 8-1 while Table 8-2 shows the descriptive statistics of the variables being studied.

Table 8-1: Profile of Organizations that Responded

Demographic	Category	Frequency (N=103)	Percentage
Country	New Zealand	44	42.7
	Malaysia	59	57.3
Number of Employees	Less than 500	3	2.9
	501 to 1000	28	27.2
	1001 to 2000	41	39.8
	More than 2000	31	30.1
Size of IT Function	No IT/IS Department	1	1.0
	1-20 personnel	13	12.6
	21-100 personnel	56	54.4
	100-250 personnel	21	20.4
	More than 250 personnel	11	10.7
	Outsourced	1	1.0
Size of InfoSec Function	No InfoSec function	25	24.3
	1-5 personnel	20	19.4
	6-10 personnel	30	29.1
	11- 20 personnel	22	21.4
	More than 20 personnel	2	1.9
	Outsourced	4	3.9
Categories of BDS Adoption	Adopter	56	54.4
	Non-Adopter	47	45.6

Table 8-2: Descriptive Statistics of Variables

Study Variables	Mean	Standard Deviation
Exogenous Constructs (Technological Context)		
Perceived Complexity (PCX)	3.23	.994
Perceived Compatibility (PCM)	3.35	.847
Exogenous Constructs (Organizational Context)		
Top Management Support (TMS)	3.40	.978
Information Security Culture (ISC)	3.45	1.03
Organizational Learning Culture (OLC)	3.55	.915
Exogenous Constructs (Environmental Context)		
Security/Privacy Regulatory Concerns (RC)	3.55	.952
Outsourcing Risks (OR)	3.46	1.02
Endogenous Construct		
Intention to Adopt BDS	3.62	1.18

8.4.2 Assessing the Measurement Model

To empirically assess the multiple-item constructs of the measurement model, confirmatory factor analyses (CFA) were conducted using partial least squares' implementation of structural equation modeling (SEM-PLS). The reliability and validity of the constructs' measures were assessed in terms of its internal consistency, indicator reliability, convergent validity and discriminant validity. Table 8-3 shows the assessment results of the measurement model.

Table 8-3: Assessment of Internal Consistency, Indicator Reliability and Convergent Validity

Constructs	Cronbach Alpha	Composite Reliability	Average Variance Extracted	Indicators	Loadings	Indicator Reliability
Perceived Complexity	0.874	0.922	0.798	PCX1	0.900	0.810
				PCX2	0.891	0.793
				PCX3	0.890	0.792
Perceived Compatibility	0.841	0.904	0.758	PCM1	0.878	0.770
				PCM2	0.873	0.762
				PCM3	0.861	0.741
Top Management Support	0.924	0.943	0.769	TMS1	0.940	0.884
				TMS2	0.838	0.702
				TMS3	0.888	0.789
				TMS4	0.820	0.672
				TMS5	0.892	0.796
Information Security Culture	0.912	0.932	0.697	ISC1	0.828	0.686
				ISC2	0.881	0.776
				ISC3	0.821	0.674
				ISC4	0.886	0.785
				ISC5	0.840	0.706
				ISC6	0.747	0.558
Organizational Learning Culture	0.730	0.818	0.532	OLC3	0.589	0.347
				OLC4	0.769	0.591
				OLC5	0.756	0.572
				OLC6	0.787	0.619
Regulatory Concerns	0.857	0.903	0.700	RC1	0.802	0.643
				RC2	0.837	0.701
				RC3	0.858	0.736
				RC4	0.848	0.719
Outsourcing Risks	0.854	0.910	0.772	OR1	0.865	0.748
				OR2	0.880	0.774
				OR3	0.891	0.794
Insignificant factors were dropped (OLC1, OLC2, OR4, OR5).						

Indicator Reliability: Indicator reliability represents the variance extracted from an item. For this model, standardised outer loadings of all 33 items were checked to ensure a value of above 0.7 (Hair, Ringle, & Sarstedt, 2011). The outer loading relevance testing was done iteratively. In the first iteration, several items' outer loading was found to be below 0.7 (OLC1, OLC2, OLC3, OR4 and OR5). Out of these 5 items, only item OLC3 was retained after the final

iteration because its removal leads to a decrease in composite reliability. Every item retained in the model has an indicator reliability of above 0.5 (the square of a standardised indicator's outer loading) except for item OLC3.

Composite Reliability: Composite reliability evaluates the internal consistency reliability of the measurement model. From the assessment, it is shown that both Cronbach Alpha and composite reliability values of the constructs are well above the cut off value 0.7 as recommended by Hair et al. (2014). Thus, all constructs have shown high levels of internal consistency reliability.

Convergent Validity and Discriminant Validity: Convergent validity determines the correlation level between a measure and alternate measures of the same construct. As shown in Table 8-3, the average variance extracted (AVE) value for all constructs are higher than 0.5, suggesting that the constructs explain more than half the variance of its indicators (Barclay, Higgins, & Hompson, 1995). Discriminant validity reflects the extent to which different constructs are distinctly diverse from each other (Hair, Black, Babin, Anderson, & Tatham, 2010). For this assessment, Fornell and Larcker's criterion were used (Fornell & Larcker, 1981). The criterion states that the square root of AVE for every construct must be larger than its correlation with other constructs. All constructs in this model fulfil the established criterion.

8.4.3 Assessing the Structural Model

After confirming that the results of all parameters tested for the measurement model were satisfactory, SEM-PLS was then used to assess the structural model. Structural model assesses the relationship between exogenous and endogenous latent variables through evaluation of path coefficients, coefficient of determination (R2), predictive relevance (Q2) and effect size (f2).

Before these assessments were made, the structural model was first evaluated for any collinearity issues.

Collinearity Assessment: To assess for any collinearity issues, tolerance level and variance inflation factor (VIF) were measured. According to Hair et al. (2014), tolerance level of below 0.20 and VIF of above 5.0 in predictor constructs are indicative of collinearity. Measured by running four separate OLS regression in SPSS (collinearity diagnostics requested), all predictor constructs' tolerance level and VIF values of the model did not meet the criterion for collinearity. Hence, collinearity among predictor constructs is not an issue in the structural model.

Path Coefficients: Path coefficients represent the hypothesized relationships among the exogenous and endogenous constructs. As can be seen in Table 8-4, 5 out of the 7 exogenous constructs have significant paths leading to the endogenous variable. *Top Management Support (TMS)* and *Information Security Culture (ISC)*, is shown to have a positive association with *Intention to Adopt BDS*. Whereas, *Perceived Complexity (PCX)*, *Regulatory Concerns (RC)* and *Outsourcing Risks (OR)* show a negative relationship. *OR* was first found to be statistically insignificant based on its path coefficient value, but after running bootstrapping technique, its *t-value* reveals that OR is in fact significant. The paths for both *Perceived Compatibility (PCM)* and *Organizational Learning Culture (OLC)* were statistically insignificant (path coefficients < 0.20).

Table 8-4: Path Coefficients with t values for the Structural Model

	Path Coefficients	***t* Values**	**Significance Levels**	**p Values**	**90% Confidence Intervals**
PCX → iAdopt	-0.320	2.509	**	0.01	[0.02, 0.53]
PCM→iAdopt	0.020	0.190	NS	0.85	[-0.16, 0.20]
TMS→iAdopt	0.222	1.814	*	0.07	[0.02, 0.42]
ISC→iAdopt	0.214	1.778	*	0.08	[0.02, 0.41]
OLC→iAdopt	0.030	0.422	NS	0.67	[-0.09, 0.15]
RC→iAdopt	-0.282	2.769	***	0.00	[0.11, 0.45]
OR→iAdopt	-0.170	2.038	**	0.04	[0.03, 0.31]
Note: *p<0.10 **p<0.05 ***p<0.01 NS=Not Significant					

Coefficient of determination (R^2) and Effect Size (f^2): The amount of variance in the endogenous construct explained by all exogenous constructs is represented by the value of R^2. Coefficient of determination is also used to measure the predictive accuracy of a model. R^2 value ranges from 0 to 1, where higher values indicate a higher predictive accuracy. Chin (1998) describes results above the value of 0.67 as being "substantial", 0.33 as "moderate" and 0.19 as "weak".

Figure 8-2 shows the model's R^2 value (0.653) which is closed to be considered as having a "substantial" predictive accuracy. Evaluation of f^2 *effect size* was also made to determine whether omission of any exogenous constructs leads to a substantive impact on the endogenous construct. The effect sizes of exogenous constructs *PCM*, *ISC*, *TMS* and *OLC* on the endogenous variable is small (less than 0.02) while the effect sizes of *PCX*, *RC* and *OR* on the endogenous construct is medium (less than 0.15) (Cohen, 2013).

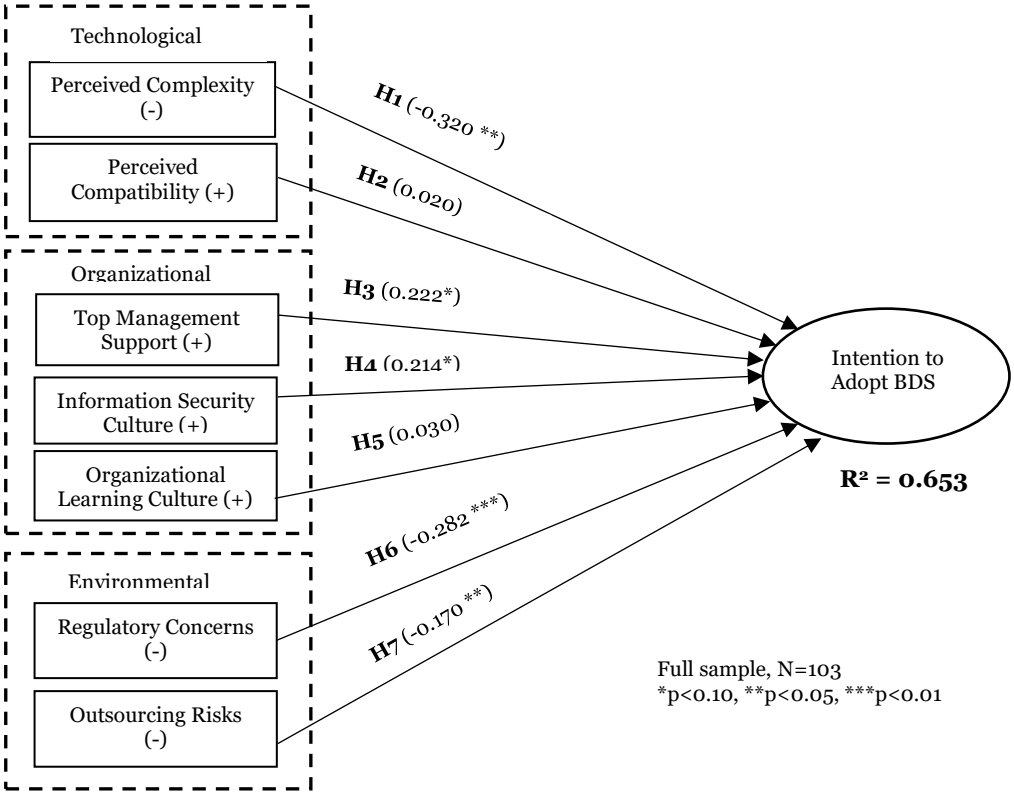


Figure 8-2: Results of PLS Analyses for the Conceptual Model

Predictive Relevance: Predictive relevance (Q^2) of the model was evaluated using Blindfolding approach. The value of cross-validated redundancy generated by the Blindfolding approach is used to validate the predictive relevance of the model. Based on Fornell and Chia (1994), a value of above zero (>0) shows a model's predictive relevance while a value of below zero (<0) illustrates a lack of it. The resulting Q^2 value is 0.6095, confirming the predictive relevance of the model.

8.5 Discussion

This study establishes the value of using TOE framework (in this case Sec-TOE) to understand security determinants in the adoption of an innovative technology – BDS. The empirical results

indicated that there are significant determinants in each technological, organizational and environmental context of the Sec-TOE framework. All seven hypotheses have been tested using the full sample (N=103) and demonstrated several findings. Interpretations based on the findings are discussed below.

8.5.1 Technological Context

Within the technological context, *perceived complexity* was found to have a significant negative influence on organizational intention to adopt BDS. As indicated by the significant and negative path in Figure 8-2, this finding supports H1 hypothesis which states organizations that perceived higher complexity in ensuring security for BDS will negatively affects its intention to adopt BDS. This also confirms that some organizations view BDS as one technological innovation that presents unique security threats and issues, thus protecting the whole BDS environment will be a highly complex process. Parallel to other research that measures the effect of complexity factor in innovative technology adoption, this finding also shows that high (perceived) complexity impedes adoption.

Unexpectedly, *perceived compatibility* was found to be statistically insignificant (p>0.10). Although it has a positive path towards intention to adopt BDS, the path coefficient and t-value do not provide support for this study's hypothesis (H2). Compatibility of organizations present security technology and mechanisms with the security requirements of BDS don't seem to be a determining factor in BDS adoption. Surveyed organizations are all public listed – larger organizations that have more resources and ability to invest in new security technologies required by BDS. That probably is the reason why compatibility is not a major determining concern in BDS adoption for these organizations.

Results for both constructs suggested that organizations are paying more attention to potential deterrent factor, i.e. *complexity*, than to a factor that may facilitate adoption, i.e. *compatibility*, when making initial decision to adopt BDS. Organizations may view BDS as a relatively new technology with unclear threats and risks, thus the reason why complexity is linked to intention to adopt BDS rather than compatibility.

8.5.2 Organizational Context

As theorized earlier, *top management support* for IS security positively affects organizations' intention in BDS adoption. The results for this construct shows a statistically significant value for both its path coefficient and *t*-value. Top management support is certainly a key factor in IS security effectiveness for organizations. Stronger management support for IS security will allow adequate financial and technical security resources to be allocated during initiation of BDS adoption. Organizations will also be more willing to identify and acknowledge security and privacy risks associated to BDS adoption. In addition, top level managers may show their support in IS security by being actively involved in formulation of security policies and monitoring of organization-wide security practices (Kankanhalli et al., 2003). Although this study focuses on security-related factors as determinants of BDS adoption, this finding is closely consistent to those of Sun et.al. (2016). Through a content analysis made based on published literatures in business intelligence and analytics, they found management support as one of the main factors that affects organizational adoption of big data (Sun et al., 2016).

With respect to the second construct in organizational context, this study's findings suggest that organizations with *information security culture* embedded in it will be positively affected in its intention to adopt BDS. This is in line with prior hypothesis made. Organizations may agree on the impact that information security culture have towards reducing security risks

associated to employees' behaviour. For an innovative technology such as BDS, the risks that comes with it may yet to be fully understood.

Thus, with embedded information security culture, employees will be more aware of potential threats in their daily job functions, especially those who are direct/indirect users of BDS. Higher concern and awareness will help to alleviate the impact of any security threats that occur during initial BDS adoption and its actual usage. Information security culture has previously been researched in different context (e.g. Singh et.al. (2014), Van Niekerk and Von Solms (2010)), this study therefore adds to the growing evidence of importance of organizational information security culture by establishing it as one of security-related factors that affects technology adoption.

Interestingly, *organizational learning culture* was found to have no effect towards intention to adopt BDS. The result of a positive path agrees with the positive direction of H5 hypothesis, but the values of both path coefficient and its *t*-value are statistically insignificant, thus it failed to provide support for H5 hypothesis. Although it is foreseen that a positive learning culture will assist organizations in learning new skills required in providing effective security for BDS, this do not seem to be a strong determining adoption factor to organizations that participated in this study. However, the mean score for this construct is 3.55 (Table 8-2), which is a higher value than *uncertain* scale (at 3.0). This score generally implies an agreement among the organizations that organizational learning culture is an important factor to information security effectiveness.

From the results above, both *top management support* and *information security culture* were found to be significant determinants in intention to adopt BDS. Among these two factors, top

management support has a statistically higher significance compared to information security culture. Hence, organizations looking to embark on big data initiatives may need to seek and ensure full support from its top management in relation to information security. With stronger support, all aspects of organizational information security will be better implemented thus creating a safer environment for BDS adoption.

8.5.3 Environmental Context

This study's findings confirm that *security and privacy regulatory concern* negatively affects intention to adopt BDS. In fact, among all constructs evaluated, security and privacy regulatory concern has the highest significant *t*-value as previously shown in Table 8-4. Security and privacy regulatory issues are particularly relevant in the use and processing of big data. In fact, big data present complex issues in relation to legal rights. Organizations with big data operations may have to perform complicated tasks of assessing whether its use of data falls outside the scope of any licensing terms or if there is non-compliance with any relevant regulations (Kemp, 2014). The challenge for organizations also include making sure that they abide to privacy principle of using data only according to its intended purpose during data collection. This is consistent with the result of one study that found the need for "having policies for privacy and security of personal data as the most pressing challenge" in big data implementation (Rehman & Qingren, 2017). Both countries surveyed for this study have its own privacy act; Privacy Act 1993 for New Zealand and Personal Data Protection Act 2010 for Malaysia. Therefore, organizations operating in both countries are expected to be aware of the requirement to comply with these acts in collecting, use, disclosing and storage of personal data. Due to these complexity and potential legal repercussion, it may dampen organizations' interest in adopting BDS.

The result for *risks in outsourcing* shows a negative path towards intention to adopt BDS and is statistically significant for both its path coefficient and *t*-value. This result supports the H7 hypothesis - risks in outsourcing negatively affects intention to adopt BDS. The underlying concern for the organizations may originate from potential risks that are often associated with outsourcing practices. Being a relatively new technology, adoption of BDS often involved outsourcing and use of third-party tools. Before selecting the vendors for outsourcing, organizations need to consider the vendors' competence, skills and approach to information security (Dhillon, Syed, & Sá-Soares, 2017). These selection criteria are crucial to ensure organizations' information assets are secured and vendors can comply with organizations' security policies, standards and processes. Lack of confidence and trust towards outsourcing vendors may contribute to organizations' hesitance in adopting solutions such as BDS. Results for both examined environmental constructs above adds to growing evidence that information security issues do not only originate from technological factor. Organizations are also concern about potential risks and issues that may arise from external environmental factors during adoption of innovative technology. Excessively limiting privacy regulations and incompetent outsourcing vendors among others, will impede the adoption of an otherwise highly beneficial technology. Accordingly, these environmental factors should be thoroughly assessed by organizations when making decision to adopt BDS.

8.6 Conclusion, Limitations and Future Work

While BDS has been hyped as an innovative technology that may provide organizations with numerous strategic and operational benefits, there are still concerns among organizations on issues related to its adoption. One of the most frequently cited hindering issue is security and privacy of big data. Consequently, it is essential to understand what security related issues that

may affect the intention to adopt BDS. Using TOE Framework, this study developed and validated a conceptual model called Sec-TOE in examining the positive/negative influence of seven factors on intention to adopt BDS.

Several key findings were obtained by this study on the security determinants in BDS adoption. These key findings are as follows: 1) Security-related technological, organizational and environmental factors may affect the intention to BDS by organizations. 2) Out of the seven examined constructs, five constructs (perceived complexity, top management support, information security culture, security and privacy regulatory concern and outsourcing risks) were found to be statistically significant security determinants in BDS adoption. 3) Among the five significant determinants, three were found to have negative influence on BDS adoption (perceived complexity, security and privacy regulatory concern, outsourcing risks), while another two determinants (top management support, information security culture) have a positive effect on BDS adoption. 4) Security and privacy regulatory concern has the highest significant value affecting organizational intention to adopt BDS followed by perceived complexity.

Additionally, this study verifies the applicability of TOE framework in understanding determinants of innovative technology adoption such as BDS. The study also featured security-related determinants in BDS adoption, which was not found in other technology adoption studies using TOE framework. One rarely examined construct in technology adoption was also introduced in this study. The construct is information security culture which was found to be a significant security-related factor that may affect technology adoption. The findings also show that organizations are more concern on the security factors that may impede BDS adoption rather than the factors that may facilitate adoption. These results therefore will be beneficial

for practitioners and organizations in understanding the security factors that need to be taken into consideration when initiating BDS adoption and which factor should be assigned the highest priority. Vendors of BDS may also utilise the results of this study to analyse their potential clients' current security capability and expectations in developing a solution tailored to the needs of the clients.

This study is not without its limitations. First, this study was conducted in two countries only; New Zealand and Malaysia. Therefore, some caution must be taken before generalizing the findings to organizations operating in different environment (for example, the issue of power distance). Generalizability of the findings may be limited to New Zealand and Malaysia-based organizations and other countries with similar operating environment; especially in Asia Pacific context. Next, the examined factors in this study were mainly extracted based on literature review, thus there may be other relevant factors not included in the conceptual model. This provides an opportunity for future research to further identify security-related technological, organizational and environmental factors that may be significant in BDS adoption.

As this is the first of a two-phase study, the plan for the next phase is to conduct a case study within a single organization to further complement the results. The second phase is meant to derive further support on how information security is viewed during adoption of innovative technology such as BDS.

9. Security Considerations in Big Data Solutions Adoption: Lessons from a Case Study on a Banking Institution (Article 5)

9.1 Introduction

At present, the massive amount of data being collected and generated daily offer various analytical opportunities for organizations to uncover information that are beneficial for its operation. This vast amount of data and its numerous analytical possibilities led to the birth of the term 'big data'. Although big data has been one of the highly discussed technologies by scholars and practitioners alike, there is no standard definition of the term itself. Hence, big data is often defined by its characteristics – the "3V's" which represent volume, variety and velocity of data (Benjelloun & Lahcen, 2015). Some scholars have also introduced the fourth "V" which characterized data veracity (Miele & Shockley, 2013). Organizations confronted with current stormy market environment are consistently looking to adopt advanced technology that can assist them in gaining competitive advantage and to build their innovative capability. The introduction of big data technologies may offer organizations with the required solution, by providing capabilities to analyze larger volume of data with greater speed and accuracy than previously possible. Thus, big data has now moved from being merely a trend to being one of the most critical innovative technology deemed adoptable by organizations. Its application and role are now widely recognized not just in businesses, but also in other sectors such as healthcare and government, encompassing various disciplines.

However, before deciding to adopt big data solutions (BDS), there are several initial decisions and measures that must be taken into consideration by organizations. Besides initial issues such

as relative advantage, cost and technical expertise, one other critical issue that must be considered by organizations deciding to adopt BDS is the issue of security and privacy (Sun et al., 2016). With the maturity of BDS, security and privacy presents serious concerns for various parties; individuals, organizations and governments, mainly due to the sheer volume of personal data being collected and analyzed. During the process of technology adoption, it is common for an organization to encounter new security threats and challenges posed by the technology. The same occurrence should be expected in the adoption of BDS. Yet, security has often been treated as an afterthought in most organizations. This can lead to security failures mainly caused by the use of inappropriate threat detection method and security mechanisms in data protection (Loukaka & Rahman, 2017). For organizations with a big data environment, security should never be treated as secondary, thus it is ideal to provide security mechanisms from the ground up instead of "adding up security to an already complex data environment as an afterthought" (Duncan et al., 2018). Organizations with an established security and privacy mechanisms in the development and use of big data will reap more desirable results and less consumer pushback (Goodendorf, 2013).

In recent years, even though security and privacy issues of big data has garnered a great deal of attention from scholars and numerous big data-related publications are available, few researchers have attempted to investigate on the security and privacy related factors that are considered during organisational BDS adoption process. Therefore, as a continuation from a previous study that identifies technological, organizational and environmental security determinants in BDS adoption, this study was intended to further develop a better understanding on how information security shape organisational BDS adoption through a single case study of a banking institution. The main research question that underpin this study is as follows*: What security-related factors are considered by organizations during the process of*

BDS adoption? The following sections of this paper starts with a brief literature review in section 9.2, followed by the research methodology in section 9.3. Next, the synthesized results are presented in section 9.4. The paper proceeds with a discussion in section 9.5, and ends with conclusion and limitations of the study in section 9.6.

9.2 Literature Review

9.2.1 Big Data and Security Issues in Organizations

Previous studies have identified possible security and privacy issues in relation to big data (Saraladevi, Pazhaniraja, Paul, Basha, & Dhavachelvan, 2015; Sharif, Cooney, Gong, & Vitek, 2015). For example, concerns that arise in the collection of sensitive and personal data by organizations which relates to privacy matters (Mennecke et al., 2014). But, data privacy is not the only concern in regards to security of big data. An organization is also vulnerable to other security threats and cyberattacks due to the wider range of data being collected and stored. Security mechanisms in organizations with big data capabilities need to be properly installed to avoid unintended security breach such as the sharing of sensitive data and information to unintended parties. Without effective security mechanisms in place, it may introduced several repercussions to an organization, among it are reputational damage and financial loss(Lee, 2017b). Lee (2017) also argues that "weak security creates user resistance to the adoption of big data".

This resistance to BDS adoption is also supported by the findings of surveys conducted by several marketing research and technology consulting companies. Consistently, security and privacy factor were cited to be one of the top hindering factors for BDS adoption in organizations (Gartner Inc, 2014; Sans Institute, 2015). In one the surveys, organizational

capability to adapt to the security requirements of BDS was found to be the second prioritized factor during initial evaluation of BDS solutions offered by data analytics vendor (IDG Enterprise, 2015).

Apart from that, due to big data's diverse function and extent of reach, organisations are exposed to far greater risks in security and privacy compared to those contributed by other traditional data analysis technologies (Nasser & Tariq, 2015). The tasks of securing a big data environment is therefore different from securing a traditional data environment. Big data security is particularly more challenging due to traditional security tools that are no longer compatible with BDS (Lane, 2014). Security tools that are originally designed to work for traditional relational-database systems are not able to scale to big data's volume, variety and velocity. Moreover, the security challenges of BDS are also contributed by the absence of security features in the initial development of the solutions (e.g. early releases of Hadoop has no default security features in place) (MIT Technology Review, 2015). The tools and solutions developed to manage big data's massive data sets are often not designed to deal with security and privacy measures (Li & Gao, 2016). Thus, organisations that have the intention to adopt BDS will need to re-examine the methods and mechanisms required to secure stored data and the whole big data environment (Lane, 2014).

Clearly, there are compelling arguments for organizations adopting BDS to carefully consider security and privacy issues that may influence its adoption. Big data's security and privacy threats hence require an organization to be fully aware of the existence of these vulnerabilities. With an organization-wide awareness, it will then be possible for an organization to prepare the security policies and mechanisms required to secure a big data environment.

9.2.2 Big Data in Banking Industry

Banking industry has consistently been cited as one of the industries that may gain the most benefit from big data. In a heat map by Gartner Inc. (Gartner, 2012) that reports on big data opportunities in vertical industries, it is shown that banking and securities industry is marked as having "very hot" opportunity to benefit from "volume of data", "veracity of data" and "software" perspectives. Adoption of BDS by the banking industry is also gaining momentum. This is supported by findings of a 2017 market research on big data done by Dresner Advisory (Dresner Advisory Services, 2017), which found that 76 percent of the respondents from financial services institutions are current users of BDS.

The banking industry operates in an environment which is known to be intensely competitive. Traditionally, banks are providing very similar financial products and services to their consumers. In the current decade where consumer demands are intensified, banks can no longer rely on strategies that focuses solely on product offerings (Cohen, Gan, Hwa, & Chong, 2007). In order to remain competitive, banks are now starting to tailor their strategies to be more customer-oriented (Bedeley & Iyer, 2014). Considering the amount of data streaming into banks from a variety of channels, it is suffice to note that banks are now in need of new means to manage their (big) data. By utilizing big data analytics and solutions, banks may reap the benefits of big data by producing analytical models based on its daily transactions, social media posts and correspondence, as well as its customer service records (Bedeley & Iyer, 2014). Through these analytical process, banks are capable to extract vital information and make informed, data-driven decisions to further develop the efficacy of its various functions (Srivastava & Gopalkrishnan, 2015). Hence, banks will be able to attract new customers and retain existing ones through customized customer experience.

Although the benefits of big data in banking industry is clear, there are some challenges that may hinder its successful adoption. Security and privacy is one of the challenges that need to be addressed by banking institutions that implements BDS. A 2018 financial services edition of a data threat report by Thales (Thales & 451 Research, 2018) shows that in relation to big data implementation, discovering the location of sensitive data within a big data environment ranks as the highest concern by U.S financial firms (37%). Whereas globally, the top concern of financial services institutions is the lack of native security frameworks or controls within a big data environment (Thales & 451 Research, 2018). Cybersecurity threats involving financial institutions are also on the rise, with many high profile reports on attacks towards multinational and local banks. In Malaysia for example, its central bank reported a (foiled) cybersecurity incident where there is an attempt to perform unauthorized fund transfers using falsified SWIFT messages (Ananthalakshmi & Bergin, 2018). Since information security risks have evolved dramatically in recent years, banking institutions are now faced with difficulties in keeping pace with security mechanisms required in managing the risks (Asian Institute of Chartered Bankers & PWC, 2018). Thus, banking institutions will need to have a 'security-at-the- forefront thinking' in order to come up with a proper security management approach when dealing with a disruptive technology such as BDS. This is essential for banks in preparing for mechanisms to detect threats and respond to security events to minimize disruption in business and avoid financial losses.

9.3 Methodology

This study is a qualitative portion of a research that seeks to identify the security determinants of BDS adoption. The first portion of the research employed questionnaire survey method to identify technological, organizational, and environmental security factors that affects

organizational intention to adopt BDS, using a conceptual framework named Sec-TOE. The results of this quantitative portion is reported in (Ahmad Salleh & Janczewski, 2018). Thus, as part of an explanatory mixed-method investigation of the research, this study was conducted using a single case study approach to allow the collection of richer and in-depth information in understanding the information security-related considerations made during BDS adoption. Case study approach was selected to answer the what and how questions of this research, and to cover relevant contextual conditions before determining these conditions are indeed relevant to phenomenon being studied (Yin, 2009).

The case study was conducted within the context of a large banking organization in Malaysia. Initially, three Malaysian banking organizations were invited to participate in the study. The three organizations were chosen based on publicly available information on their adoption of BDS in supporting parts of their operation. This purposive sampling method is to ensure the selection of an organization that has a clear understanding on BDS adoption and its associated security factors before and after implementation. Out of the three, one organization responded and agreed to take part in the case study. The case-study organization is a large banking organization in Malaysia with a regional presence in Singapore, Hong Kong, Vietnam, Cambodia and China. In Malaysia alone, the bank has an extensive network of more than 200 branches. The banking organization utilizes BDS in what they term as “cognitive computing” in analyzing customer profiles, reports and product information in identifying customers’ needs. In return, customers are offered available financial services that suits them. The implemented BDS is capable to analyze both structured and unstructured data and presents the analytics through visualization. Data protection and cybersecurity mechanisms of the bank are applied at all locations but the main decision making for overall information security

infrastructure and technology adoption are centralized at the bank's corporate headquarters in Malaysia's capital.

The primary data collection technique used in the case study is semi-structured interview with several relevant employees of the banking organization. The interview technique was employed to derive employee's interpretation of their organizational BDS adoption and information security experiences and their understanding of them. In total, interviews were conducted with 7 employees with different designation and job scope. The differing roles and job scope are to ensure a collection of data from different perspectives.

But, careful consideration was made to ensure all interviewees has a direct knowledge on the organization's BDS adoption process and/or are users of the analytical products of the BDS. All interviews were conducted in a duration of one month (in May 2018). Most interview sessions were conducted face-to-face (2 interviews were conducted using telephone), and lasted for around 45 – 60 minutes.

Before the start of each interview, all interviewees were given a 'participants information pack' which include participant information sheet, background of the study and interview guidelines/protocol (also consist of 12 key questions guide). In essence, the interviewees were asked on what security and privacy challenges they would consider during BDS adoption. Interviewees at the 'user' level were also asked on how the bank enforces data protection policy. All interviews were recorded and transcribed in verbatim in preparation for analysis stage. The background details of the interviewees are presented in Table 9-1.

Table 9-1: Profile of Interviewees

Employee ID	Role of Interviewees	Years in Organization
E1	Head of Group Security	3
E2	Head of Analytics Infrastructure and Technology	5
E3	IT Security Manager	13
E4	Strategic Analytics Manager	4
E5	Senior Executive – Business Intelligence	5
E6	Senior Executive – Customer Analytics	3
E7	Executive – Customer Analytics	3

Secondary data collection technique used was public documentation reviews. Publicly available documentation related to the banking organization such as its recent annual report, sustainability report, security policies, news articles and any other relevant information obtainable from the banking group's website were reviewed to provide another source of evidences. The review also helped in preparing for the interview sessions by facilitating formulation of key and follow-up questions.

9.4 Analysis and Results

The analysis stage of the study mainly employs thematic analysis (Boyatzis, 1998) which involves the process of coding to identify themes, sub-themes and patterns. The identification of main themes was guided by a conceptual framework introduced in the first quantitative portion of the research (the Sec-TOE framework). This framework is adapted from an organizational-level technology adoption framework - TOE framework (DePietro et al., 1990), and used to investigate how seven security-related constructs affects organizational intention in adopting BDS. The three main themes are 1) technological security-related considerations, 2) organizational security-related considerations, and 3) environmental security-related considerations. Utilizing both primary and secondary sources of data collection, data

triangulation were performed whenever possible during analysis. A qualitative data analysis software (NVivo) was used to organize and analyze all transcribed interview, memos, and public documentation gathered during the data collection process. As a result of the analysis process, the findings were organized into three main themes and sub-themes as shown in Table 9-2 below:

Table 9-2: Themes and Sub-Themes Derived from the Study

Themes	Sub-themes
Technological security-related considerations in BDS adoption	Challenges in securing data Capability of legacy security measures
Organizational security-related considerations in BDS adoption	Managerial information security awareness Top management support for security resources Security education, training and awareness (SETA) Security personnel skills and experience Employees perception on sensitivity of information assets
Environmental security-related consideration in BDS adoption	Regulatory compliance Reputation of BDS vendors Environmental uncertainties

9.4.1 Technological Security-related Considerations in BDS Adoption

Challenges in securing data: Generally, the large volume of data generated by the bank is not seen as a recent phenomenon by the participants, as they are aware that the bank have traditionally been operating with large volume of data. However, with the introduction of new technological trends such as big data and its diverse data-centric solutions, there are some uncertainties around how these data are handled, where are the data stored, and how will it be

secured. Challenges in securing data was identified as one of the factors being considered during the bank's BDS adoption process. This is reflected in the answer by E3:

> *"When we were considering jumping on the big data bandwagon, one of my main concern is …whether we need new data protection mechanism. Yes, for sure, we have always maintain the security of our data assets, it's just that with big data, the level of protection needed is more robust. I mean, the plan is to have customer experiences monitored, so there has to be a high level of trust"*.

Whereas, E1 agreed with the complexity and challenges of securing data, but is confident that their security team is able to come up with a comprehensive security policy that caters to big data environment. He stated,

> *"Complexity in securing big data is one of the factors that we think of during adoption process. Now that there's a growing concern on data exfiltration…especially with the many forms of data that we are dealing with. Observation and effective analysis is key. I'm confident our security team will be prepared with the right foundational control and measures".*

Capability of legacy security measures: The capability of the bank's legacy security measures is another technology related consideration derived from the interviews. To several of the participants, the security measures that they have in place before the start of their big data initiative may no longer be sufficient to address the new infrastructure. Quoted from participant E1:

> *"Big data tech… when paired with cloud architecture may pose a challenge for our legacy security measures. Its capability to scale to big data's security need for*

> *example…lack of it will lead to multiple security concerns. We had to revise our security approach…introduced new security measures, make sure the new infrastructure is properly protected".*

Mostly, feedback from participants with security background shows that they view the need to consider the capabilities of legacy security measures in protecting big data environment as an important process – especially in maintaining the bank's security profile.

9.4.2 Organizational Security-related Considerations in BDS Adoption

Managerial information security awareness: Since BDS is a relatively new technology and may present various security and privacy issues, it is therefore essential for an organization adopting it to have a high-level of information security awareness (ISA). While this notion is generally agreed by participants, several of them mentioned that before the bank can achieve an organization-wide awareness, the top management itself must have a sensible perception on information security and privacy. As stated by E6,

> *"We will do all the necessary actions required from us, but I guess we'll only do what we're told to do. Training or tests... orders must first come from the management. Security awareness need to start with them".*

Top management support for security resources: Top management support has been found to have a positive impact on technology adoption decisions in many research. In this study, the same result holds, where most participants agreed that the process of BDS adoption went smoothly due to top management support. When the bank's top management championed the move towards digital business model transformation, one of the pre-set goals is to increase

customer satisfaction by harnessing the power of digital capabilities and big data analytics. As noted by several participants, the goal to leverage big data is clearly communicated to relevant parties in the bank, suggesting full support from the top management on BDS adoption. Participant E1, expected top management's support in BDS utilization to translate into support towards security-related requirements and resources needed for protecting a big data environment. The two participants with security background assert that every projects including BDS adoption require both security and risk assessments, in order to conform to existing rules and compliance requirement. Hence, having support from the top management level is essential to ensure security planning is aligned with the outcome of assessments and the bank's digital transformation plan, apart from *"having an adequate funding budgeted for security" (E3).*

Security education, training and awareness (SETA): Based on the responses of the participants, security education, training and awareness was among the identified factors being considered in BDS adoption. Several participants believe that in order to reduce security risks for new technology implementation (in this case - BDS), the bank will need to formulate a detailed plan in educating and creating security awareness among different stakeholders dealing with the technology (either directly or indirectly). Participant E4 commented as following,

> *"The bank has always treated awareness as a key theme in security. So what we do here are...e-based awareness program for cybersecurity and private data protection, online training, among others. All are meant to facilitate communication and security education".*

It is interesting to note that one participant from the 'user' level (E7) emphasized that they (the employees) will not know what is expected of them in terms of conforming to security and privacy requirements in the use of BDS, unless the bank explicitly create the awareness through targeted communication and training program.

Security personnel skills and experience: Some of the security concerns around BDS adoption are related to uncertainties in security threats brought upon by BDS deployment. For example, the "variety" and distributed nature of big data, which will make it more difficult to protect. From the interviews, it emerged that several participants observed current InfoSec professionals as having increasingly complex and evolving threats to deal with. They relate these concerns with the need for highly skilled and experienced security personnel to help the bank navigate potential threats and uncertainties of big data. Participant E3 for instance, acknowledged that*;*

> *"....on the matter of security, it is possible to solve and deal with threats…problems…or any shortcomings, as long as we have the right people on the job. Right people with the right skills and experience in network security and system security"*.

A few of the participants also point out on "big data skills gap" that may make it harder to overcome security challenges.

Employees' perception on sensitivity of information assets*:* Responses from managerial-level participants indicate that employees' perception and behavior towards information sensitivity is an important aspect to be considered during BDS adoption. They unanimously

agreed that the bank's employees' behavior may pose risks to information protection such as data breaches that started internally. A statement by participant E2 sums up the said concern*:*

> *"I believe that human factor is one of the biggest threats to information security. We can never be complacent with the current measures we have in place…well, there must be a continuous effort to inculcate security thinking (as a culture)"*.

As they are a banking institution's employees, their use of BDS in enhancing customers' experience will also involve customers' privacy and confidentiality. Consequently, their perceptions and behavior towards information security need to be one that understood the nature, confidentiality and sensitivity of information.

9.4.3 Environmental Security-related Considerations in BDS Adoption

Regulatory compliance: Apart from complying with acts that are meant to regulate and supervise banking institutions, payment systems, and other relevant entities, banks that capitalizes on BDS will also have to abide to other security and privacy-related regulations. Regulatory compliance was identified as one of the main considerations in BDS adoption by the participants. Almost all of them mentioned the need to comply with regulations and acts as stipulated by the Central Bank of Malaysia (BNM) and other governing bodies. Some of them specifically mentioned that they are faced with extra responsibilities and requirements in ensuring compliance with Malaysia's Personal Data Protection Act 2010 (PDPA). Participant E1 for example, states that:

> "*Well…complying with PDPA… we had to do a lot of things….audits on personal data types, privacy policy, introduced a framework for PDPA compliance…training staff on the workings of PDPA…to name a few. We are one of the 11 sectors mandated to register under the Act, so we do our best to comply with all PDP principles, although it can be challenging with big data"*.

Staffs working closely with customers (hence customer personal data), are also tested on their knowledge of these Acts for compliance purposes. As specified by participant E6,

> *"Once a year, we have to sit for tests that relates to compliance with PDPA, AMLA, Islamic Finance…and several others. We have to know all basic principles to ensure we met the compliance requirement".*

Most participants also agreed that the main challenge is to be able to respond quickly to changes in regulations, primarily because they are operating in a dynamic regulatory environment.

Reputation of BDS vendors: Another factor for consideration derived from the interviews is the issue of vendor reputation. Two of the participants have had a direct role in selection of vendor for their first BDS venture. They suggest that vendor reputation will have a direct role in ensuring the security of their big data. Among the identified security-related vendor criteria considered by the participants are; transparency of vendor's security architecture, and vendor acceptance towards external audit/assessment on their security measures and processes. Participants E2 provides the following statement*:*

> *"....since big data is relatively new to us…we need vendors that have good reputation….market leading names. Those with transparency, willing to work closely with us in safeguarding our data assets…and of course vendors with strong financial means and resources".*

Participant E1 affirms that reputation of vendor in big data arena was among the main selection factor, especially when the bank was among the first financial institutions in Malaysia that embark on big data initiative,

> *"…we considered on established reputation of the service providers…besides conducting security due diligence during the selection process".*

Environmental Uncertainties: Several participants expressed their concern on the news of large-scale data breaches that occurred in Malaysia. These news gave them the outlook and possibilities of big data-related insecurity and uncertainties. Participant E3 for example, believes that the environment in which the bank operates in presents increasingly hazardous threats and uncertainties*:*

> *"News of data breaches…fairly recently the news of cyberattack on BNM, it is to me a wake-up call for banks to re-examine our cybersecurity efforts. We considered multiple issues…threats from outside the bank when we're planning for our big data initiative. We do not want to make a wrong decision that leads to failure even before the system reaches its maturity stage."*

They are aware that the factor of environmental uncertainties must be met with proper planning and preparation to avoid repercussions. As stated by participant E5,

> *"Uncertainties in various areas are to be expected with new technology…so we need to have a solid plan, protect our assets and reputation. We have to retain our customers, and we are likely to attract new customers based on our reputation."*

9.5 Discussion

In the previous section, results synthesized from the case study were presented. From the results, it can be seen that there are various security related considerations made by the banking institution in the process of adopting BDS. The issues being considered show that security matters do play a role in organizational BDS adoption. From technological perspective, two security-related issues were found to be the central considerations made by the bank. The issues of challenges in securing data and capability of legacy security measures are consistent with the findings of other surveys that found complex data environments as the top hurdle to data security besides inadequate traditional solutions (Benjelloun & Lahcen, 2015; IDC, 2019). Therefore, awareness and understanding of these issues is important in adoption decision. Organizations need to identify its weaknesses in relation to securing a big data environment and be able to continuously evolve in order to match with constantly changing threat factors. Organizations planning to adopt BDS must not be complacent with their current security mechanisms or assume that what they have are sufficient for protecting a complex big data environment.

From organizational perspective, five security-related issues were identified as the main considerations in BDS adoption by the bank. Managerial information security awareness, top

management support for security resources, SETA, security personnel skills and experience, and employee's perception on sensitivity of information assets are all important aspects that may have an effect towards the successfulness of BDS implementation. This is in line with several studies that found management awareness, visibility and active participation are needed in formulating effective information security policies (ISP) and other information security-related efforts during new technology adoption (Choi, Kim, Goo, & Whitmore, 2008; Haeussinger & Kranz, 2017; Kankanhalli et al., 2003). These considerations draw attention to the role of top management in instilling an organization wide security awareness, especially when dealing with data intensive technology such as BDS. It is important to note that this awareness and support towards security must start from the top management to ease all efforts in security planning and management of BDS.

As for environmental perspective, this study found that there are three security-related considerations made by the bank during the process of BDS adoption. One issue that was identified in this study and regularly appeared in technology adoption research is the issue of regulatory compliance (Ahmad Salleh & Janczewski, 2018). It was acknowledged by the participants that compliance toward security and privacy related regulations has become more challenging with big data. Regulatory compliance is crucial for industries that works with a large amount of personal data such as the banking industry, thus this may be the reason why compliance issues were brought up by the participants. In addition to compliance consideration, this study also found that BDS vendor reputation and environmental uncertainties as among the issues being considered during BDS adoption. These three issues would be a good starting point for consideration by organizations during risks assessment process in BDS adoption. Organizations will have to identify their ability in complying with security and privacy regulations, and their readiness in responding to threats posed by environmental uncertainties.

9.6 Conclusion and Limitation of Study

This study is an attempt to explore the security-related considerations made by an organization during BDS adoption through a single case study of a banking institution. Grounded on TOE framework in identification of the main themes, this study has shown that the security considerations may be divided into three contexts; technological, organizational, and environmental. The identified main security issues for considerations were: challenges in securing data, capability of legacy security mechanisms, managerial security awareness, top management support, SETA, security personnel skills and experience, employees' perception on sensitivity of information assets, regulatory compliance, reputation of BDS vendors and environmental uncertainties. These findings provide values to big data, information security, and technology adoption research domain. It would also be beneficial for security managers and organizations in formulating better security-related strategies in BDS adoption.

Although the use of a case study may provide richer understanding on the security considerations made during BDS adoption process, it may limit the ability to generalize the findings due to; 1) use of a single case study, and 2) case study is of a single industry. Future studies may consider to use multiple case studies conducted across various industries to allow for more reliable comparisons between industries.

10. Security Determinants in the Adoption of Big Data Solutions: A Mixed-Method Approach (Article 6)

10.1 Introduction and Background of Study

Big data is a term that has garnered much attention in this decade and its values have gained recognition by multiple industries and governments. Many businesses have started to transform from being a traditionally operated business to digitizing most of their work processes in order to produce new products and services. Efficient use of big data may transform these businesses by providing opportunities to mine huge volume of data and perform analytical process at a speed that was not previously possible (Baig et al., 2019). With these opportunities, businesses may enter new market at accelerated speed, and armed with new solutions to improve their competitive advantage (Sun et al., 2016).

Big data is not just about massive volume of data. Initially, big data is characterized by its "3Vs" characteristics; the volume, velocity and variety of data (Perera et al., 2015). Now, some researchers have extended its characteristics to "5Vs", with the addition of veracity and value (Li & Gao, 2016). In response to the birth of big data, many technology providers have developed new and powerful computing solutions that are able to process big data's volume and its other unique characteristics. The advancement of these solutions may contribute significantly to adopting organizations. For example, big data solutions (BDS) that equipped organizations with the ability to generate analytical insights for new approaches in marketing strategies, production, supply chain, customer relationship, and in several other business areas (Mazzei & Noble, 2017).

While big data is promoted as having great transformational values, organizations seeking to adopt the solutions must first take into considerations several issues that may affect its successful implementation (Raguseo, 2018). Prior assessments and strategic decisions are important and must be made at organizational level before the start of adoption process especially when it involves a new technology innovation such as BDS. One of the issues that has been acknowledged in relation to big data adoption is the issue of security and privacy (Al-qirim et al., 2017; Liu & Greene, 2020). It is widely known that with the current era of extensive connectivity, the amount of data generated has increased immensely in volume, and data are being produced at a greater velocity. This incredible speed in generating huge volume of data brought upon numerous security and privacy threats and challenges (Park & Kim, 2019). In addition, the varied format of data and multiplicity of platforms typical in a big data environment also magnify the challenges to ensure data security and privacy.

Empirically, the issue of security and privacy has consistently appeared as one of the most prevalent challenges in BDS adoption. In a systematic review done by Frizzo-Barker et.al. (2016) on big data in business scholarship, it was found that data privacy risks and other data-related security issues are the second most prevalent challenges for businesses. Similar issues were also encountered in a report of a survey done by Dataguise (2016), which revealed that around 73% of surveyed enterprises' big data initiative were either delayed or terminated in response to data security concerns. These findings are indication that security challenges create resistance towards BDS adoption. Else, due to big data's distinctive security and privacy challenges, Lu et.al. (2014) argued that if organizations failed to appropriately address these challenges, it will likely be detrimental to big data's widespread acceptance.

Although the number of big data related literatures are huge, there have been little attempt among researchers to understand the factors that may affect organizational intention in BDS

adoption (Chen et al., 2016; Nguyen & Petersen, 2017). Presently available research conducted on big data adoption mainly concentrated on general influencing factors of adoption. Among these literatures, very few provided a closer look on specific issues identified as having an influence on BDS adoption (e.g. security and privacy). Hence, based on current interest in big data investment and implementation by organizations, it is therefore timely to study on the factors that may influence organizational adoption of BDS. This study aims to contribute to available literature by providing empirical evidence on the technological, organizational, and environmental security and privacy factors that may affect the intention to adopt BDS, and security and privacy factors that are being considered by adopting organizations. Grounded in the Technology-Organizational-Environmental (TOE) framework (DePietro et al., 1990), this study identified the factors through a sequential explanatory mixed-method study consisting of a survey analysis on a sample of 103 organizations in New Zealand and Malaysia, and a single case study on a Malaysian banking institution. The outcome of the study is meant to develop a better understanding for both researchers and practitioners on security and privacy factors involved in BDS adoption.

The following sections in this paper are organized as follows: section 10.2 presents the theoretical background, and the next section 10.3 presents the two methods used in the study. This is followed by section 10.4, which presents the results and findings for both studies. Section 10.5 is a discussion section that integrates the findings of both phases of the study. The paper ends with a conclusion and limitations of the research in section 10.6.

10.2 Theoretical Background

As previously mentioned, this study utilizes the TOE framework as the main theoretical framework guiding the research process for both quantitative and qualitative phases. TOE

framework was introduced in a book chapter co-authored by DePietro, Wiarda and Fleischer in 1990. The framework consists of three main contexts that are said to influence the process of technology adoption and implementation at organizational level. The three contexts are; *technological*, *organizational*, and *environmental*.

The first context - the *technological* context, refers to both internal and external technologies relevant to the firm (DePietro et al., 1990). Technology in this context may represent both equipment and processes. The main focus related to this context is on how technology characteristics may influence innovation adoption process (Chau & Tam, 1997). For the quantitative phase of this research, two constructs were used: *perceived complexity*, which refers to the technological complexity of ensuring security of BDS, and *perceived compatibility*, which refers to compatibility of current security technology of an organization to address the security concerns and threats of BDS.

The next context in the framework is *organizational*. This context refers to multiple characteristics that represent a firm in general such as organizational strategies, culture, structure as well as policies (Teo et al., 2006). It may also refer to the size of an organization, the scope of its business, and its managerial structure that could have an effect in the organizational technology adoption. These characteristics may either be a facilitating factor in adoption or a limiting factor (Oliveira & Martins, 2011; Teo et al., 2006). By looking at the factors from security perspective, the constructs that were identified and adapted for this research are, *top management support* that denotes the level of support and commitment given by organization's top management towards IS security requirement and mechanisms involved in BDS adoption. The second construct is *information security culture*, which refers to organizational efforts in relation to information security practices, and the third construct is

organizational learning culture – referring to the ability or processes in an organization that enables and promotes learning of new skills.

The third context is *environmental*. It refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" (DePietro et al., 1990). Influences coming from the environment in which the organization operates may become external factors that could affect technology adoption. This include clients, suppliers, competitors, government policies and regulations related to an organization. Two constructs were used for this research; 1) *regulatory concern* (level of concern organizations have toward the requirement to comply with security and privacy regulations) and, 2) *risks of outsourcing* (outsource BDS or use of third-party tools). The following are the list of hypotheses generated in identifying seven security-related constructs that may facilitate or hinder organizational intention to adopt BDS.

Technological Context

H1: Higher perceived complexity in ensuring the security of BDS negatively affects organization's intention to adopt BDS.

H2: Perceived compatibility of organization's present security technology and mechanisms with security requirements of BDS positively affects organization's intention to adopt BDS.

Organizational Context

H3: Top management support for IS security positively affects organization's intention to adopt BDS.

H4: Embedded information security culture within organizations positively affects organization's intention to adopt of BDS.

H5: Positive organizational learning culture positively affects organization's intention to adopt BDS.

Environmental Context

H6: Security and privacy regulatory concern negatively affects organization's intention to adopt BDS.

H7: Risks in outsourcing negatively affects organization's intention to adopt BDS.

Besides being adopted as the main framework for the quantitative phase of this study, the TOE framework was also used as a guidance in identifying the main themes and sub-themes of the qualitative (case study) phase.

10.3 Methodology

This study employs a sequential explanatory mixed-method approach. The approach implies the "collection and analysis of first quantitative data and then qualitative data in two consecutive phases in one study" (Ivankova et al., 2006). The primary objectives of this study are to identify the security and privacy factors that may affect the intention to adopt BDS, and security factors that are being considered in the adoption process of BDS. It is also meant to provide an integrative understanding of the issues from both quantitative and qualitative studies. The study follows a set of design procedures for sequential explanatory mixed-methods approach as suggested by Ivankova et.al. (2006).

10.3.1 Study 1 – Quantitative Phase

For the first phase of the research, a quantitative study was conducted using cross-sectional survey method. The goal for this quantitative phase was to identify the security determinants in organizational intention to adopt BDS. A conceptual model was developed to examine seven security-related constructs (within three main contexts: technological, organizational, and environmental) that may affect the intention to adopt BDS. All constructs in the conceptual model are measured using security and privacy related indicator items thus the model is named as Sec-TOE.

Constructs in the Survey

Development of constructs in the model were based on a comprehensive review on information security and technology adoption literatures. All constructs were measured using security-related indicator items, which differ from the common indicator items used in measuring constructs of other technology adoption studies that uses the TOE framework. Hence, most of the indicator items were adapted from findings or statements in previous studies especially in the area of information security. Every constructs (*perceived complexity (PCX), perceived compatibility (PCM), top management support (TMS), organizational learning culture (OLC), information security culture (ISC), security and privacy regulatory concern (RC), risks in outsourcing (OR)*) were operationalized as reflective constructs and have a total of 32 indicator items. The endogenous construct (*Intention to Adopt BDS*) was also operationalized as reflective and was measured using 2 indicator items adapted from (Teo, Wei, & Benbasat, 2003). These indicator items were then measured using a 5-point scale that ranges from 1=Strongly Disagree to 5=Strongly Agree.

Preliminary Survey

Before the actual survey was administered to target respondents, a preliminary survey was conducted to test the survey instrument and to derive a preliminary result. The target respondents for this preliminary survey were the members of New Zealand Information Security Forum (NZISF), which is New Zealand's information security special interest group. From this preliminary survey, some amendments were made to several indicator items based on the suggestions and comments received from the respondents. Initial results derived from this preliminary survey was reported in Ahmad Salleh and Janczewski (2016).

Actual Survey

The survey packages containing a questionnaire were sent out together with a cover letter, invitation note, participant information sheet, consent form, and a prepaid reply envelope to 353 identified CIO/CEO's of public listed organizations in both New Zealand and Malaysia. Contact information were gathered from NZX company research database and Bursa Malaysia. The reason why public listed organizations were chosen as the sampling frame for this survey is due the high probability that these organizations generate high volume of data (big data) and may have an interest in initiating big data investment. As the survey's unit of analysis is organization, an instruction was given to the recipients, to select one respondent that may best represent their organization – those that has the knowledge on the organization's technology adoption practices, and/or information security practices and policies. As an alternative to the mailed package, an online questionnaire was also created using an online survey tool (Qualtrics).

In total, 117 responses were gathered through mail and the online survey tool (52 from New Zealand and 65 from Malaysia). Next, the returned surveys were checked for consistency. 14

invalid responses were dropped which produced a final dataset of 103 responses. The final dataset consists of 44 responses from New Zealand and 59 responses Malaysia. This leads to a final response rate of 29.1%. All necessary tests were conducted on the final dataset to check for potential biases (due to the two-country data), and common method bias was also tested using Harman's one factor test (Podsakoff et al., 2003). The results show that there were no significant biases found for the two countries and the dataset did not possess any issues with common method bias (variance explained by a single factor is 21.065%). Thus, it is safe to conclude that the survey methodology does not contribute to any significant biases to the dataset.

Data Analyses

The analysis stage was conducted in 3 steps, 1) a preliminary analysis done to identify any biases and to generate descriptive statistics, 2) measurement model assessment, and 3) structural model assessment.

For *preliminary analysis*, the dataset was analyzed and screened to check for anomalies. Identified monotone responses were then deleted and this was followed with a missing value analysis. Using Little's MCAR test, it was found that the missing value occurred randomly, therefore replacement of the missing values was done using Expectation Maximization (EM) technique. Normality check done using the Shapiro-Wilk test revealed a p value less than chosen alpha level of 0.05 ($p<0.01$), which rejected the normality hypothesis of the test. To check for differences between the countries, Mann-Whitney U test was done and the derived asymptotic significance level was 0.459 ($p>0.05$). This result shows that the dataset does not have statistically significant evidence of differences between New Zealand and Malaysia in its

median intention to adopt BDS. Thus, the combined dataset was then used in succeeding assessments of the measurement model and structural model.

Majority of the respondents are the staffs and managers in IS/IT department (48), followed by IS security staff and management (23), head of business units/departments (16), CIOs (8) and another 8 respondents from other categories of job functions. Consumer goods, retail, and financial services represent the three largest industries that responded to the survey. Table 10-1 presents the demographic characteristics of the responding organization.

Table 10-1: Demographic Characteristics of the Respondents

Demographic	**Category**	**Frequency**
Country	New Zealand Malaysia	44 59
Number of Employees	Less than 500 501 to 1000 1001 to 2000 More than 2000	3 28 41 31
Size of IT Function	No IT/IS Department 1-20 personnel 21-100 personnel 100-250 personnel More than 250 personnel Outsourced	1 13 56 21 11 1
Size of InfoSec Function	No InfoSec function 1-5 personnel 6-10 personnel 11- 20 personnel More than 20 personnel Outsourced	25 20 30 22 2 4
Categories of BDS Adoption	Adopter Non-Adopter	56 47

The analysis of the measurement model and structural model will be discussed in the next section (in *findings*).

10.3.2 Study 2 – Qualitative Phase

For the second phase of the research, a single case study on a banking institution was carried out by using interviews as the main technique for data collection. This second phase qualitative study was done to assist in elaborating the quantitative results obtained in the first phase (Ivankova et al., 2006). The central aim for this second phase is to derive an understanding on the security and privacy related considerations made by organization in the process of BDS adoption.

The Case Institution

Invitation to participate in the case study was first sent out to three Malaysian banking institutions. Out of the three, one large banking institution replied and agreed to participate. The banking institution is known to have adopted BDS in supporting parts of their operation. Due to this, it can be ensured that the bank have had an experience and understanding on BDS adoption as well as security and privacy related considerations involved in the adoption process. The bank is the fifth largest banking institution in Malaysia with an extensive network of close to 300 branches across the country. The bank also has a presence in several other Southeast Asian countries such as Singapore, Vietnam, and Cambodia as well as in East Asian countries (Hong Kong and China).

The BDS deployed in the bank is able to monitor experiences of customers in utilising the bank's products and services through sophisticated analytical and social media capabilities. As a result of this monitoring and analytics, the bank is able to plan their customer service strategies and cross-selling of products. The bank also believes that by having this automated

technology with big data, they may transform their customers' experience by offering predictive and more intuitive services.

Data Collection Technique

The data collection for the case study was mainly conducted using semi-structured interviews. The interview technique was used in order to seek richer evidences on the employees' understanding of the bank's information security experiences and involvement in BDS adoption. In total, 7 employees of the bank participated in the interviews which occurred in a timeframe of one month in May 2018. The seven participants have different job scope and designation but all have either a direct knowledge on the bank's BDS adoption process or the direct user of the resources derived from the BDS.

Interviews were conducted face-to-face except for 2 sessions which were conducted using telephone. Each interview sessions lasted around 45-60 minutes. The interviews were audiotaped (with the consent of the participants) and later transcribed in verbatim. All seven participants received a "participant information pack" that provides information on the study's background, interview guidelines, and key questions guide (which was grounded in the first phase's quantitative results) before the agreed date of their interview sessions.

The interview questions mainly revolve around security and privacy challenges and considerations in BDS adoption as viewed by the participants. Participants were also asked on the method that the bank use in enforcing data protection and privacy policy. The following Table 10-2 shows the profile of the seven participants.

Table 10-2: Profile of the Interviewees

Employee ID	Role of Interviewees	Years in Organization
E1	Head of Group Security	3
E2	Head of Analytics Infrastructure and	5
E3	IT Security Manager	13
E4	Strategic Analytics Manager	4
E5	Senior Executive – Business Intelligence	5
E6	Senior Executive – Customer Analytics	3
E7	Executive – Customer Analytics	3

Secondary data collection technique was also used in the case study. Among others, public documents available about the bank were reviewed, such as its annual report, annual sustainability report, security policies, news articles and other relevant information gathered from the bank's official website. The researchers also made reflection and field notes to help in the case description.

Data Analysis

Thematic analysis (Boyatzis, 1998) was conducted on the collected data with the help of qualitative data analysis software- NVivo. The software was used to store all transcribed data, notes, memos and public documentation gathered during the data collection stage. The software was also used in coding and theme identification. The thematic analysis involved several steps of coding, identifying themes, sub-themes and patterns. As the case study is in sequence to the first phase survey, the identification of the main themes was grounded in the main framework used in the survey – the Sec-TOE Framework. For verification purposes, both primary and secondary data were triangulated, interviews were richly described, and subthemes were reviewed to resolve any inconsistencies. The findings from this analysis stage is discussed in the next section (results and findings).

10.3.3 Integration of Results from Both Phases of the Study

After acquiring the results from both phases of the study, the next stage involve integration of these results to form the final outcome of the entire study. Integration refers to a stage in mixed-method approach where the results generated from both quantitative stage and qualitative stage are mixed or integrated (Creswell & Clark, 2011; Ivankova et al., 2006). This process is also known as meta-inferences (Venkatesh et al., 2013). Integration normally forms the last stage of a mixed-method approach.

The integration of the results are presented in the discussion of the outcomes of the entire study in later section, whereas detailed results of each phases has been reported in (Ahmad Salleh & Janczewski, 2018) and (Ahmad Salleh & Janczewski, 2019). Finally, this integrative analysis resulted in a revised Sec- TOE framework for BDS adoption.

The following Figure 10-1 shows a visual model of the study's Sequential Explanatory Mixed-Methods Design Procedures.

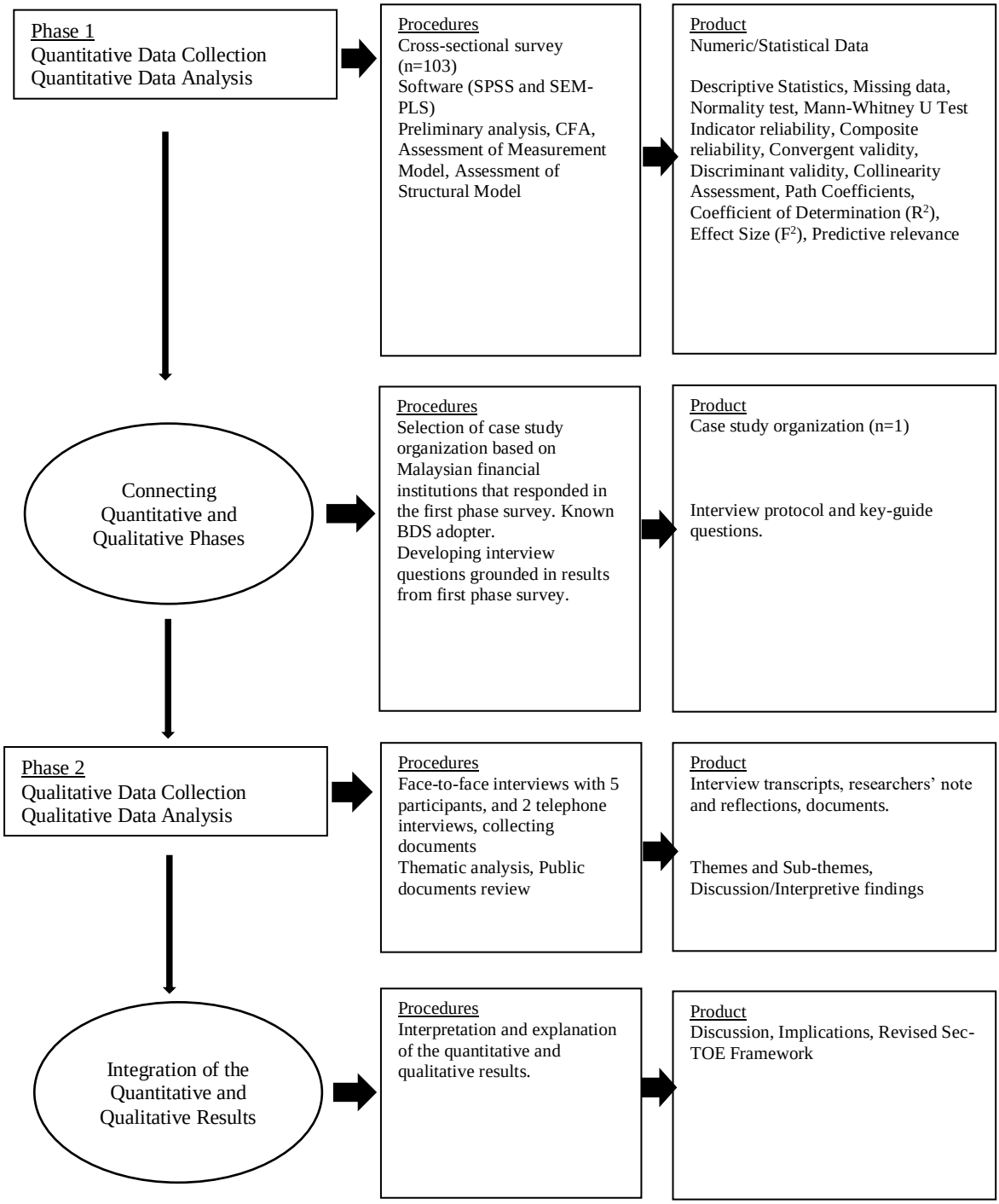


Figure 10-1: Visual Model for the Study's Sequential Explanatory Mixed-Methods Design Procedures

10.4 Results and Findings

This section presents the results and findings of both the quantitative and qualitative studies. For the first phase study, results of the assessment done on the measurement and structural model will be presented. This is followed with a brief discussion on the findings of the second phase single case study.

10.4.1 Study 1 – Findings of Quantitative Phase

For assessment of the measurement and structural model, partial least square implementation of structural equation modelling (SEM-PLS) was used following the guidelines by Hair et.al. (2014). The PLS method was selected for analyzing the conceptual model due to the non-normality of the dataset and the explorative nature of the study (Hair, Hult, Ringle, & Sarstedt, 2014). For the first step, a Confirmatory Factor Analysis (CFA) was conducted using SmartPLS software to assess the measurement model. This is done to compute internal consistency, indicator reliability, convergent and discriminant validity of the constructs' measures.

Table 10-3 shows the standardized outer loading and indicator reliability of the model's indicator items. The outer loading relevance test was done in iteration to ensure that all items retained are those having a suggested value of above 0.7 (Joe F. Hair et al., 2011). After the final iteration, items OLC1, OLC2, OR4 and OR5 were removed from the model (loadings below 0.7). Item OLC3 (loading= 0.589) was retained because its removal decreases composite reliability. The indicator reliability values of all retained items exceed the minimum acceptable value of 0.4 and close or greater than the preferred level of 0.7 (except for item OLC3 with indicator reliability of 0.347) (Hulland, 1999).

Table 10-3: Indicator Reliability

Indicators	Loadings	Indicator Reliability
PCX1	0.900	0.810
PCX2	0.891	0.793
PCX3	0.890	0.792
PCM1	0.878	0.770
PCM2	0.873	0.762
PCM3	0.861	0.741
TMS1	0.940	0.884
TMS2	0.838	0.702
TMS3	0.888	0.789
TMS4	0.820	0.672
TMS5	0.892	0.796
ISC1	0.828	0.686
ISC2	0.881	0.776
ISC3	0.821	0.674
ISC4	0.886	0.785
ISC5	0.840	0.706
ISC6	0.747	0.558
OLC3	0.589	0.347
OLC4	0.769	0.591
OLC5	0.756	0.572
OLC6	0.787	0.619
RC1	0.802	0.643
RC2	0.837	0.701
RC3	0.858	0.736
RC4	0.848	0.719
OR1	0.865	0.748
OR2	0.880	0.774
OR3	0.891	0.794

Table 10-4 shows the assessment for composite reliability, convergent validity and discriminant validity. For composite reliability, all values are well above the recommended threshold of 0.7 thus demonstrating the internal consistency of all constructs (Hair et al., 2014). The average variance extracted (AVE) value of all measured constructs are found to be higher than 0.5 which suggests that the constructs explain more than half its variance of its indicators (Barclay et al., 1995). Discriminant validity was then analyzed using the Fornell-Larcker criterion which results illustrate that the square root of AVE for every construct is greater than its correlation with other constructs in the model (Fornell & Larcker, 1981). In overall, convergent and discriminant validity can be assumed for the measurement model.

Table 10-4: Quality criteria for the Constructs

Constructs	Cronbach Alpha	Composite Reliability	Average Variance Extracted (AVE)
Perceived Complexity (PCX)	0.874	0.922	0.798
Perceived Compatibility (PCM)	0.841	0.904	0.758
Top Management Support (TMS)	0.924	0.943	0.769
Information Security Culture (ISC)	0.912	0.932	0.697
Organizational Learning Culture (OLC)	0.730	0.818	0.532
Regulatory Concerns (RC)	0.857	0.903	0.700
Outsourcing Risks (OR)	0.854	0.910	0.772

Next, several tests were conducted to assess the structural model. As a start, test for collinearity issues was conducted by measuring the tolerance level and variance inflation factor (VIF) using OLS regression in SPSS. All predictor constructs' tolerance level exceed the value 0.2 and its VIF are all below the recommended threshold of 5.0 (Hair et al., 2014). Thus, the structural model did not display any collinearity issues among the constructs. The path coefficients were then calculated based on the PLS method and bootstrapping procedure. It was found that 5 out of the 7 exogenous constructs have a significant path towards the endogenous variable. The 5 constructs are PCX, TMS, ISC, RC, and OR (OR found significant after bootstrapping). With path coefficient level of less than 0.2 (p<0.2), PCM and OLC were considered as statistically insignificant. The results of this test is summarized in Table 10-5.

Coefficient of determination (R^2) of the model is 0.653, suggesting a close to "substantial" predictive accuracy according categories proposed by Chin (1998). The effect size (f^2) was also evaluated to see if there is any substantive effect towards the endogenous construct when any of the exogenous constructs were removed. Based on Cohen (2013), it was found that the effect size towards endogenous construct is small (less than 0.02) for PCM, ISC, TMS and OLC, whereas the f^2 is medium (less than 0.15) for PCX, RC and OR. Finally, predictive relevance (Q^2) of the model was evaluated using Blindfolding approach. The generated value of cross validated redundancy was 0.6095 thus confirming the predictive relevance of the model.

Table 10-5: Results for Structural Modelling Assessment

	Path Coefficients	*t* Values	Significance Levels	*p* Values	90% Confidence Intervals	Results for Hypothesis
PCX→ iAdopt	-0.320	2.509	**	0.01	[0.02, 0.53]	Supported
PCM→iAdopt	0.020	0.190	NS	0.85	[-0.16, 0.20]	Not supported
TMS→iAdopt	0.222	1.814	*	0.07	[0.02, 0.42]	Supported
ISC→iAdopt	0.214	1.778	*	0.08	[0.02, 0.41]	Supported
OLC→iAdopt	0.030	0.422	NS	0.67	[-0.09, 0.15]	Not supported
RC→iAdopt	-0.282	2.769	***	0.00	[0.11, 0.45]	Supported
OR→iAdopt	-0.170	2.038	**	0.04	[0.03, 0.31]	Supported
Note: *p<0.10 **p<0.05 ***p<0.01 NS=Not Significant						

10.4.2 Study 2 – Findings of Qualitative Phase

Based on the thematic analysis conducted which were grounded in the Sec-TOE framework, three main themes were identified; 1) technological security-related considerations 2) organizational security-related considerations, and 3) environmental security-related considerations.

Table 10-6: Themes and Sub-Themes Derived from the Study

Themes	Sub-themes
Technological security-related considerations in BDS adoption	Challenges in securing data Capability of legacy security measures
Organizational security-related considerations in BDS adoption	Managerial information security awareness Top management support for security resources Security education, training and awareness (SETA) Security personnel skills and experience Employees perception on sensitivity of information assets
Environmental security-related consideration in BDS adoption	Regulatory compliance Reputation of BDS vendors Environmental uncertainties

The analysis process resulted in ten sub-themes besides the three identified main themes as depicted in Table 10-6. As has been stated in the methodology section, the full report on the

findings of the second phase study has been reported in (Ahmad Salleh & Janczewski, 2019), thus this section will only discuss the derived themes and sub-themes briefly.

For technological security-related considerations in BDS adoption theme, two sub-themes were identified from the analysis. The participants seem to agree that one of the considerations made during the bank's BDS adoption process is *challenges in securing data*. There is a common agreement among the respondents with security background (E1 and E3) that BDS adoption will contribute to complexity in securing data and it may require the bank to deploy a new data protection mechanism. Despite this concern, the respondents maintain that they have always ensure that the bank's data asset are well protected and with BDS, they are confident that their security team will be prepared to confront any security issues with the right "foundational control and measures" (E1). Another consideration derived from the interviews is the issue of *capability of legacy security measures*. Several participants believe that the security measures that they have in place pre-BDS may not be able to scale to security needs of BDS environment. They consider that BDS deployed on cloud platform (as the bank's BDS is) would introduce new security concerns that will require a revised security approach and measures. Generally, the participants viewed the need to evaluate the bank's legacy security measures as an important step in protecting BDS environment. This is to avoid any security breach that may harm the reputation of the bank.

Five sub-themes were derived under organizational security-related considerations. The first consideration is *managerial information security awareness*. Almost all interviewed participants agreed that with new technology such as BDS, there needs to be a high level of information security awareness (ISA) that essentially, needs to start from the managerial and top management level. Participant E6 for example, believe that the awareness must start from the top management as they (lower level executives) would only perform necessary actions

required when orders are given by the management. The next consideration is *top management support for security resources.* Majority of the participants note that the bank's top management clearly communicated the decision to embark on big data initiatives, signalling a support for any big data-related requirements. One participant (E1), expected this support given by the top management towards BDS adoption to translate into support towards security resources requirements in safeguarding a big data environment. The support is needed in order to have "adequate funding budgeted for security" (E3). It is also crucial in ensuring development of a security plan that is aligned with the outcome of risks assessments conducted for BDS adoption. *Security education, training and awareness (SETA)* is another organizational issue derived from the analysis. Participants mainly consider a detailed plan in educating and creating security awareness is required in reducing security risks associated with new technology adoption. Different stakeholders who deals with BDS directly or indirectly need to conform to security and privacy requirements of BDS, and this may be facilitated by targeted communication and training program (E7).

Further, *security personnel skills and experience* was also seen as one important consideration during BDS adoption process. Some participants observed that current threats that are more complex and evolving will be a burden for InfoSec professionals. Thus, the main concern is to have experienced and highly skilled security personnel to assist the bank in navigating the uncertainties and potential threats contributed by the use of BDS. The fifth sub-theme derived for organizational security-related considerations is *employees' perception on sensitivity of information assets*. Participants at managerial level pointed out that this issue is an important consideration that needs to be made during BDS adoption. They believe that employees perception and behaviour towards information assets is key in determining the effectiveness of security mechanisms applied by the bank. Behaviour and negative security perception of

employees may pose risks to any data protection efforts – for example, data breaches that may be intentionally/unintentionally initiated internally by ignorant employees.

Under environmental security-related considerations, the issue of *regulatory compliance* was among the identified concerns in BDS adoption. Majority of the participants talked about how it is compulsory for them to abide to various regulation stipulated by the Central Bank of Malaysia and other governing bodies. Some of them specifically mentioned that it became tougher to abide to privacy act such as Malaysia's Personal Data Protection Act 2010 (PDPA) with the use of BDS. For example, they have to perform audits on personal data types, trainings, and develop new framework for PDPA compliance (E1). Another interesting consideration identified in the study is the issue of *vendor reputation*. Two of the participants have had a direct role in BDS vendor selection process, and they both agree that reputation of vendors will play a role in ensuring the security of the bank's big data. They mentioned the need to have vendors with good reputation - those that are transparent about their own security architecture and are open to external audits on their security measures. Being among the first banking institutions in Malaysia to embark on big data initiative, they consider vendor's reputation as one of the main selection factors apart from conducting security due diligence (E1). The participants also revealed their concerns on *environmental uncertainties*. News of large scale security breaches that occurred in banking industries, especially the ones that happened locally gave them the possibilities of insecurities lead by big data. One participant (E3) believes that the bank's current operating environment presents an increasingly complex threats and uncertainties. These uncertainties were among the considerations made during the bank's BDS adoption process. There is an awareness that they need to consider external threats, re-examine their cybersecurity efforts (E3), and came up with a solid plan to protect their assets and reputation (E5).

10.5 Discussion and Recommendations

In this research, theoretically-based security determinants in BDS adoption framework was proposed based on analysis and review of relevant literature. Individually and collectively, information gathered from both quantitative and qualitative data analyses, provided insights regarding security and privacy factors influencing organizational intention in BDS adoption, and security and privacy issues being considered by organization adopting BDS. From the survey, it was found that 5 out of the 7 security and privacy factors have a statistically significant path to intention to adopt BDS. The significant factors were: *perceived complexity, top management support, information security culture, regulatory concern,* and *outsourcing risks.*

Perceived complexity was the first factor found to have an influence towards organizational intention to adopt BDS. The result shows a negative significant path, illustrating that this factor may negatively affect organizational intention to adopt BDS. From the viewpoint of this research, *perceived complexity* represent the level of difficulties in ensuring the security of a BDS as perceived by an organization. This finding shows that organizations that have the intention to adopt and/or have adopted BDS perceived that implementation of security measures is highly complex for a BDS environment. To corroborate this finding, one of the security considerations made by the banking institution in the case study was on the issue of challenges in securing data. The general perception from this banking institution was that there are uncertainties in terms on what they need to deal with in a BDS environment – for example, new requirements to introduce a comprehensive security policy tailored for BDS. They acknowledged that the process of securing data in a BDS environment is complex and challenging which require effective analysis and the right foundational control and measures. Although this case institution is a BDS adopter, the concern towards the complexity of ensuring

the security of big data provided an indication that this issue is/or can be a deterring factor in BDS adoption. This finding is also in line with the findings of a research done on big data adoption in Norway where security was perceived as challenging especially for companies in initiation stage of big data adoption (Nguyen & Petersen, 2017). While *perceived compatibility* of organizations present security technology and mechanisms with the security requirements of BDS was found to be a statistically insignificant determining factor for intention to adopt BDS, it is interesting to note that from the case study, it was one of the security issues considered during adoption. The issue relates to the capability of the banking institution's legacy security measures to scale to big data's security need and requirements. The above factors are security-related technology factors that may affect organizational intention to adopt BDS, hence it is recommended for organizations to first categorize security and data privacy as an area that requires immediate enhancement. In order for a BDS environment to be effectively secured, immediate actions need to be taken especially in identifying gaps in current security infrastructure and skills of security professionals. By addressing the identified gaps, it will have a positive impact towards sustainability of organizational BDS investment.

For security-related organizational issues, it was found that *top management support*, *and information security culture* have a statistically significant positive influence on intention to adopt BDS. Top management support in this research context refers to support from the top management towards IS security. As has been established in other technology adoption research, top management support is crucial in ensuring successfulness of an innovative technology adoption initiatives (Borgman et al., 2013). This fact also applies to top management support towards IS security and its requirements. By having the support needed, sufficient financial and resources may be channelled for all security efforts involved in BDS adoption. Top management support for security resources was also one of themes derived from

the case study. Top management are expected to clearly communicate their goals in BDS adoption along with clear support towards any requirements for security measures and resources. The case study also reveals that having support from the top management is crucial in ensuring security planning for big data initiatives is appropriately aligned with the outcome of security and risk assessments. Also, having top management support will assist in addressing the issue of security personnel skills and experience required in support of a big data environment. Security personnel need to be highly skilled, thus may require top management support for additional training in preparation to navigate associated threats contributed by BDS.

Information security culture was also found to have a positive influence towards intention to adopt BDS. From the case study, several security related considerations made by the case institution were found to be associated with information security culture. The first was the issue of managerial information security awareness which pointed to the need for the top management to have an awareness on security and privacy aspects involved in daily operations of an organization. Since any big data environment requires a high level of security awareness organization-wide, this awareness need to start with the top management. Employees of the case institution felt that in order for an organization to have the required level of awareness, the top management must demonstrate that they are aware of any security-related threats or issues linked to big data. With this, any further security education, training, and awareness programs meant for the employees of an organization will be efficiently communicated and designed. Else, it is also important for an organization to monitor employees' perception and behavior towards information sensitivity. It is important due to the possibility of security breaches that may be caused by employees' behaviour or actions that undermines the sensitivity of data and information.

Based on the above security-related organizational factors in BDS adoption, several recommendations can be made. First, an organization may focus on internal ethics, integrity, and compliance. There must be a commitment to instil security ethics and integrity within the organization. When this is achieved and information security culture are embedded as part of organizational culture, adherence to values, principles, standards, and security norms can be expected from all stakeholders involved. Second, security awareness must be made as one of the key themes in security management planning of an organization, and employees must be trained to handle current and future challenges associated to big data. One example is to have a dedicated section in organizations' website that educate employees and customers on the significance of data secrecy and associated regulation or act that governs the collection, use and disclosure of personal data. Initiatives on compliance must also be present in an organization. Again, to ensure compliance, ethics and integrity goals may be included as part compliance initiatives.

Under environmental security-related context, two factors were found to have statistically significant negative influence towards intention to adopt BDS. The two issues were *regulatory concerns* and *outsourcing risks*. In support of this findings, the case study conducted also identified similar themes where the case institution was found to have made considerations on regulatory compliance and reputation of BDS vendors. The first quantitative part of this research posited that security and privacy regulatory concern may negatively affect the intention to adopt BDS. Data privacy and protection act may be detrimental to BDS adoption due to constraints and extra responsibilities required in ensuring compliance. From the viewpoint of an adopter (the case institution), this is true especially in relation to big data. They found that it is challenging to comply with all the requirements of Malaysia's Personal Data Protection Act (PDPA) where they need to introduce a new framework specifically for PDPA

compliance. The challenge also includes the ability to promptly respond to changes in regulations. On the issue of outsourcing risks, the case institution also provided a similar response, where they consider the reputation of BDS vendors as one of the determining factor for vendor selection. The respondents viewed vendors with good reputation, are open with security assessments, and transparent with their security architecture, as the ones that will be able to ensure the security of their BDS. There are security risks which are normally associated with outsourcing practices and use of third-party tools, thus, some organizations may be deterred by this fact. Besides the two issues above, it was also found from the case study that organizations may be affected by environmental uncertainties such as global trend in security threats and data breaches.

For this environmental context, the following suggestions can be made: 1) an organization need to have compliance officers and/or representatives that provide advises on regulatory compliance. 2) to have penalties for employees that was found to be non-compliant with enforced regulations, 3) vendor assessment with a tender review committee that perform diligence reviews of suppliers' strengths in terms of financial, performance, security capabilities, and disaster recovery. To ease the concern on environmental uncertainties, it is advisable to form a security/cyber threat intelligence team that aims to increase awareness on global security threats and ability to counter these threats.

Based on the above findings and discussion, the following Figure 10-2 shows the integration of results from both quantitative and qualitative phases.

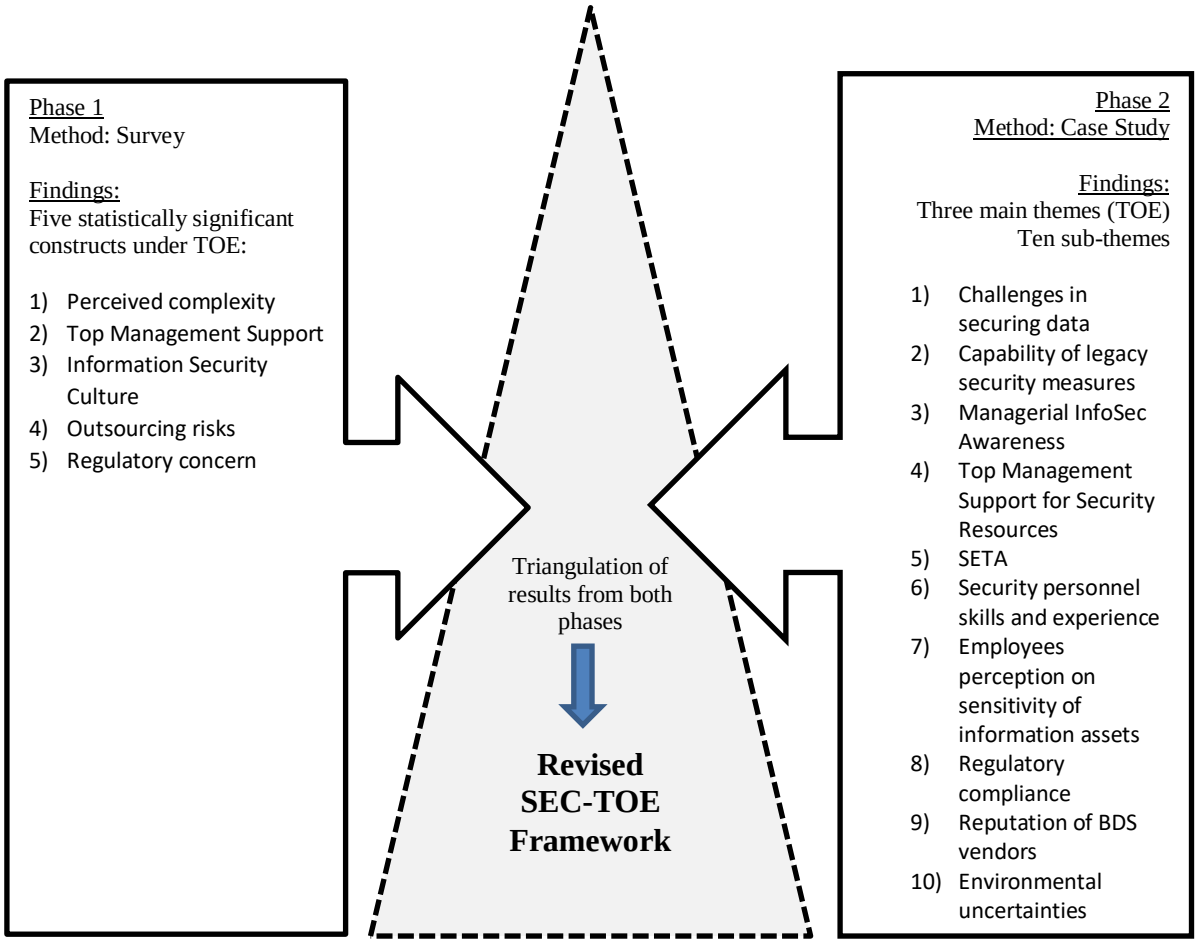


Figure 10-2: Integration of Quantitative and Qualitative Results (Triangulation)

This integration resulted in a revised Sec-TOE framework for security determinants in BDS adoption as presented in Figure 10-3.

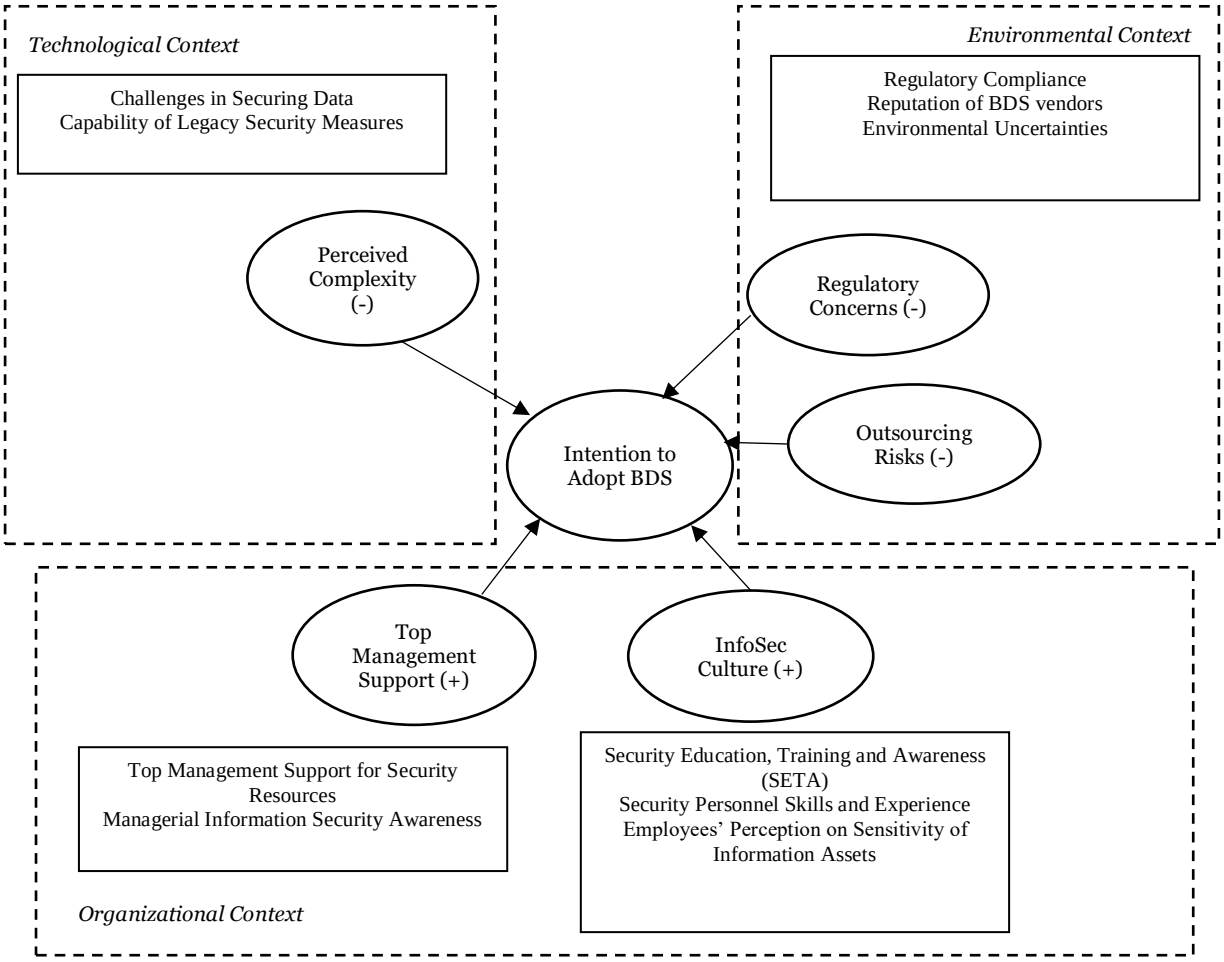


Figure 10-3: Revised Conceptual Framework of Security Determinants in BDS Adoption (Sec-TOE)

10.6 Conclusion and Limitations of Study

This research has produced a conceptual framework for security determinants in BDS adoption (Sec-TOE). The revised framework was developed based on the findings of a sequential explanatory mixed-method study which involved two data collection phases; quantitative survey followed by a single case study on a banking institution. Out of the seven constructs and hypothesis tested during the first phase survey, five were found to be statistically significant; perceived complexity, top management support, information security culture,

regulatory concern, and outsourcing risks. These findings were then complemented with results from single case study in a Malaysian banking institution. Three main themes and ten sub-themes of security consideration made by organization in BDS adoption were identified from the thematic analysis process. The findings of this second-phase qualitative were then triangulated with the findings of the survey, which resulted in the final discussion, recommendations and the revised conceptual framework. This framework is expected to contribute to academic research domain in the area of big data, security, and technology adoption; in addition to practical contributions to business organizations with an interest in BDS adoption.

Among the identified limitation of this study is; the data collection of the first phase survey involved only two countries (New Zealand and Malaysia). This fact may lead to inadequacy in generalizing the findings to organizations operating in other countries. Another limitation was contributed by the selection of a single case organization in Malaysia. Due to it being a single case study, generalizability of the findings derived from this phase may be limited to organizations operating in a similar environment.

11. CONCLUSION

This multi-paper thesis has proposed and explored theoretical security determinants in BDS adoption model that was developed to identify security-related technological, organizational, and environmental factors that affects the intention to adopt BDS by organizations. In total, there were 5 research questions developed and explored following the three main stages (*exploration, analysis, and outcome*) of the research conceptual framework. All findings related to the five main research questions were presented as six original articles found in Chapters 5-10 (Article 1 – Article 6). The aim of this final chapter is to conclude on the key findings of this research, contributions and practical implications, limitations, and directions for future studies.

11.1 Summary and Key Findings of the Research

The IT domain is currently undergoing extremely rapid growth. Newly developed technologies, applications, and managerial practices are constantly being introduced in today's digital world. The research presented in this thesis on the other hand, is the outcome of research work spanning a period of 5 years. Hence, the findings from earliest stages of the research should be assessed through the lens of the situation prevailing at the time the research was conducted, rather than from the lens of current reality.

All methodological procedures involved in this research were organized within a conceptual framework that was earlier presented in Chapter 4 (presented here again as Figure 11 -1). This conceptual framework consists of three main stages; *exploration*, *analysis*, and *outcome*. This section summarizes the key findings from each of the three main stages.

The first stage in the conceptual framework is *exploration.* The aim of this stage was to identify and understand the phenomenon for investigation, and to perform an initial investigation on the phenomenon. At this stage, the researcher started the research process assuming that there are security and privacy related factors that could affect organizations' intention to adopt BDS. In identifying and understanding the phenomenon further, a thorough literature review was done, and this resulted in the identification of six security and privacy issues related to big data.

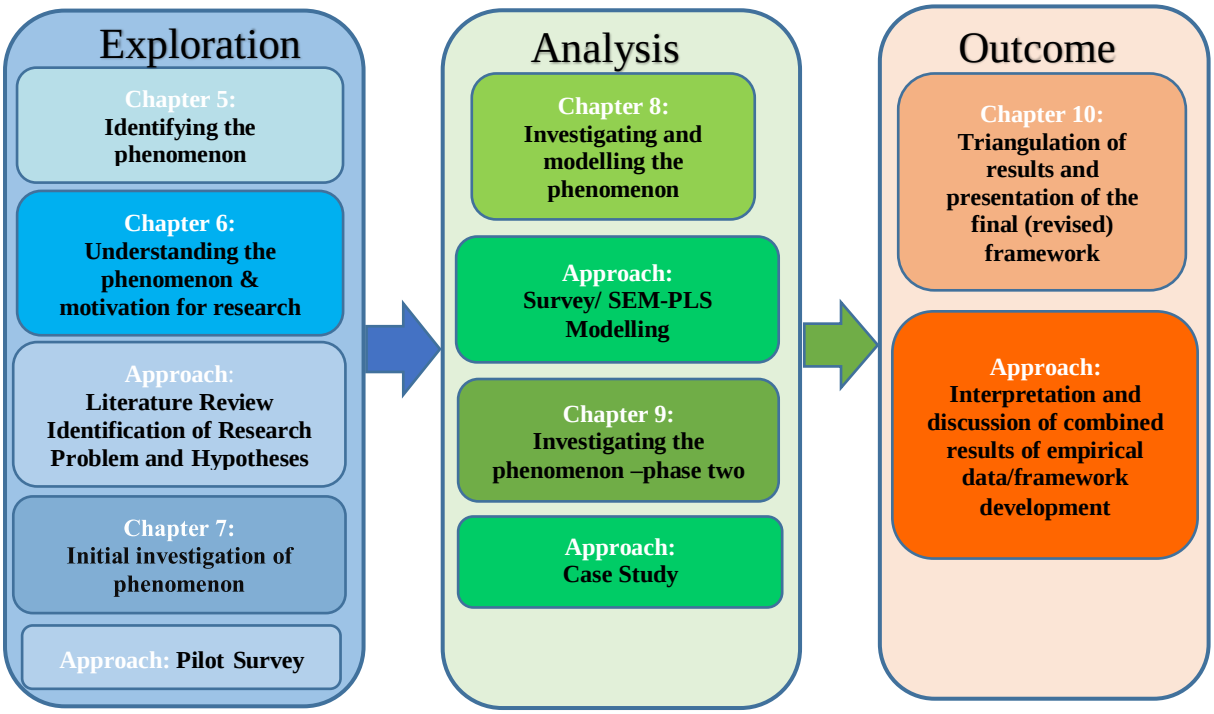


Figure 11-1: Conceptual Framework of the Thesis

The issues identified were *security and privacy technological complexity, security and privacy technological compatibility, organizational learning culture and competencies, information security culture and top management support, privacy regulatory concern,* and the final issue was *risks in outsourcing and use of third-party tools*. The above findings provided answers for

the following Research Question 1: *What are the main themes of big data's security and privacy related issues?*

The exploratory stage then moved to the subsequent research process that included an introduction to the objectives of the research, scope setting, a discussion on the theoretical foundation, development of hypotheses, and introduction of the theoretical model. This is when all six themes identified earlier were used to form seven security-related factors in BDS adoption intention of the Sec-TOE framework (*InfoSec culture* and *top management support* were treated as separate factors). The introduction and setting of research boundary during this phase produced the following main objectives of this research:

1) *To develop a conceptual security-based BDS adoption framework as a guidance for organizations planning to embark on big data initiatives.*

2) *To examine the security determinants by focusing on the influence that various security technologies, organizational security view and security related environmental factors have on BDS adoption.*

3) *To ascertain the security and privacy-related considerations made by organizations in the process of BDS adoption.*

For the final step in the exploratory stage, the researcher developed a survey instrument to test the 7 hypotheses introduced in Article 2. This survey instrument was tested through a pilot study and the results of this initial investigation was reported in Article 3. It provided answers to the following Research Question 2:

How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption among adopter and non-adopter organizations?

Adopter and non-adopter organizations were found to have differing factors that either positively or negatively affect their intention to adopt BDS. BDS adopters were found to have a relatively high agreement towards the following positive-effect factors: *perceived compatibility*, *top management support*, *information security culture* and *organizational learning culture*. Non-adopters were found to be negatively affected by *perceived complexity*, and *risks in outsourcing*.

The next stage of the research was the *analysis* stage. This stage consists of two main investigations and analyses – in line with the two phases of data collection in a sequential explanatory mixed-method approach. The first quantitative investigation involved a survey and the outcome of this survey was reported in Article 4. The research question associated with this phase (Research Question 3) and its key findings are as follows:

How do technology factors in security, organizational security view, and security-related environmental factors encourage/discourage organizations' big data solution adoption?

Based on the results from PLS analyses, it was found that there was significant positive influence arising from *top management support* and *information security culture* towards organizational intention to adopt BDS. Another two facilitating factors for adoption; *perceived compatibility*, and *organizational learning culture*, were found to be statistically insignificant.

All three hypothesized adoption deterring factors; *perceived complexity*, *security/privacy regulatory concern*, and *outsourcing risks* were found to be statistically significant. This survey also confirmed the applicability of the Sec-TOE framework in studying determining factors for technology adoption.

The next phase of the *analysis* stage was the qualitative investigation. A single case study was conducted to develop a deeper understanding of the information security issues that arose during BDS adoption process, and how information security shapes the BDS adoption in organizations. The case study using a banking institution found that considerations like *challenges in securing data*, and the *capability of legacy security mechanisms* played a key role during the process of deciding BDS adoption. Other key considerations were *managerial security awareness, top management support*, *security education, training and awareness (SETA), security personnel skills and experience*, *employees' perception on sensitivity of information assets* (all were organizational security-related considerations). Whilst, the environmental security-related considerations were *regulatory compliance*, *reputation of BDS vendors* and *environmental uncertainties*. These findings provided additional information on security-related issues that need to be considered during the BDS adoption process. Article 5 was written to report on the outcome of this phase which provided answers to the following Research Question 4:

Do organizations consider security-related factors during BDS adoption and if so, what considerations are made?

In the third stage – *outcome*, the researcher made a triangulation of results from both quantitative and qualitative data. This stage resulted in a revised Sec-TOE theoretical

framework of BDS adoption which combined the results of both quantitative and qualitative studies into one final framework. The outcome of this triangulation/integration process was reported in Article 6 which provided answers for the following Research Question 5:

What recommendations on security-related determinants can be introduced for organizations adopting big data solutions?

After completing all the necessary steps for the *exploration*, *analysis*, and *outcome* stages, this thesis managed to explore the use of TOE framework in identifying factors in BDS adoption and introduced security-related measurement items and constructs (Sec-TOE). In addition, security determinants in BDS adoption were identified, and further security-related issues and considerations made by organization during the BDS adoption process were identified. Finally, a security determinant in BDS adoption model is presented. The following Table 11-1 provides a summary of the research problem, the specific research objective, and the five research questions posed by this research.

Table 11-1: Summary of the Research Problem, Research Objective and Research Questions

Research Problem	There is a need for organizations that have the intention to adopt BDS to be aware of the security related factors that may positively or negatively affect the intention to adopt. This awareness is needed to strengthen organizational security preparation during the whole process of BDS adoption and assimilation.	**Article number**
Main Research Objective	To provide a conceptual security based BDS adoption framework as a guide for organizations planning to embark on big data initiatives.	
Research Question 1	What are the main themes related to big data's security and privacy issues?	Article 1
Research Question 2	How do technology factors in security, organizational security view, and security-related environmental factors differ in encouraging or discouraging BDS adoption amongst adopter and non-adopter organizations?	Article 3
Research Question 3	How do technology factors in security, organizational security view, and security-related environmental factors encourage/discourage organizations' big data solution adoption?	Article 4
Research Question 4	Do organizations consider security-related factors during BDS adoption and if so, what considerations are made?	Article 5
Research Question 5	What recommendations on security-related determinants can be introduced for organizations adopting big data solutions?	Article 6

Answers provided for all research questions in this thesis may benefit both academic researchers as well as practitioners as discussed in the following section.

11.2 Contributions to Research and Practical Implications

This section offers a summary of several contributions made by this research in addition to practical implications of the research findings. Following are the contributions made from the perspective of academic research:

Firstly, this thesis has served as one of the earliest empirical studies that was theoretically informed, which studied the technological, organizational, and environmental security-related determinants in BDS adoption. This thesis also expanded the use of TOE framework to address security-related constructs in studying innovative technology adoption, thus validating the applicability of the TOE framework in studying diverse organizational technology adoption. The adapted Sec-TOE framework introduced in this research is probably the first framework that was tailored to specifically examine and highlight security-related constructs only, in relation to technology adoption. It contributes to the area of information security by adding another applicable framework for hypothesis testing when studying security issues in organizations.

Secondly, this thesis has presented a systematic literature review that has identified security and privacy related issues in big data. These issues were then classified into a classification framework with three main contexts; security and privacy issues in technological, organizational, and environmental contexts. The findings of this literature review may be used for other research in the domain of big data especially in terms of informing researchers about issues that relate to big data's security and privacy. Most of big data's security and privacy issues discussed in academic research nowadays are mostly concentrated on the technical aspects of big data that may lead to security concerns. This research provided an extended view

by identifying security and privacy issues that exist as part of organizational operational practice, as well as those that exist in the environment that organizations are operating from. It is therefore appropriate to focus on security and privacy as part of technology adoption research efforts.

Thirdly, this research provides a security determinant in the BDS adoption framework that may assist organizations in identifying factors that may facilitate or inhibit BDS adoption. Researchers may use this framework to further enhance research conducted in the area of technology adoption, organizational research, and information security. The current pool of literature in big data is filled with studies that described tools, techniques, algorithms for analytic process, and general issues associated with big data's unique characteristics. This research contributed by addressing the lack of literature in BDS adoption that can provide insights into factors that may influence the adoption of BDS (specifically in terms of security related factors). The Sec-TOE framework discussed in this research is generic enough to allow for empirical testing which is also applicable for other types of technology adoption hence providing value to future studies.

Fourthly, this research has used the sequential explanatory mixed-method approach in addition to organizing the phases/steps into a research conceptual framework with three main stages: exploration, analysis, and outcome. The triangulation of results of both quantitative and qualitative studies, have resulted in a revised Sec-TOE framework that includes the security-related issues being considered during BDS adoption in addition to the security factors that may affect BDS adoption. The results of this triangulation and the revised adoption framework presented provide researchers with a holistic viewpoint on security and privacy related issues in BDS adoption formed by theoretical and empirical perspectives.

This research also has several practical implications. First, the Sec-TOE framework may provide further understanding to managers and security professionals on specific security and privacy related issues that may affect organizational intention with regards to BDS adoption. By having a better understanding of the role played by security issues in any intention to adopt and armed with the knowledge that these issues may be technological, organizational, or contributed by the environment, managers and decision makers in organizations can target, prioritize, and better allocate their security resources according to the need of a BDS environment. As the findings of this research have demonstrated that security issues may negatively affect BDS adoption, top management contemplating adoption of BDS will have to acknowledge that security is an area that needs continuous attention right from the start of the adoption process. Managers should also be encouraged to complement any big data initiatives with improved security measures, provide security-based training tailored to big data, and have a dedicated security team. Essentially, managers and other related professionals involved in any big data initiatives should be cautious as to not consider security as an afterthought. New technology such as BDS requires employees, users, and security professionals to have specific knowledge and skills, besides heightened awareness on security aspects, hence, management needs to ensure necessary training and awareness programs are provided.

Another segment of practitioners that may benefit from the findings of this research are IT service providers/vendors specifically those that offer solutions for big data. As noted in our research, one of the security-related factors that may negatively affect intention to adopt BDS is the issue of outsourcing risks. With this information, service providers could prepare a comprehensive proposal for potential BDS adopters outlining their strengths in terms of security competence, training capabilities, and technical support. Security will be among the

key concerns that potential adopters have in mind when selecting BDS, therefore, service providers/vendor may capitalize on this by offering the best solutions with effective security assurances.

11.3 Limitations and Future Work

This section summarizes the limitations and provides future research directions within areas related to this thesis. First, there are limitations which are related to the initial data collection technique namely the survey. The constructs used in the Sec-TOE framework were derived from a systematic literature review and heavily supported by theoretical considerations of previous related work that used the same TOE framework. Although the security-related constructs used were derived from this literature review process, there is a possibility that there are other relevant constructs that were excluded due to the period of published literature selected for the review process at the start of this research. However, during the process of operationalizing these constructs, there was a careful attempt by the researcher to use variables that have been previously validated and applied in other research studies. Measurement items for new constructs introduced in the Sec-TOE framework such as information security culture, and organizational learning culture, were pieced together based on a variety of past studies and may affect content validity and item reliability. For this purpose, the researcher relied on statistical measurements provided by SEM-PLS to ensure statistically irrelevant measurement items were removed before assessing the structural model. These novel constructs developed for this research may benefit from further research and theoretical development in related areas.

Secondly, the data collected for the survey were based on two countries only, New Zealand and Malaysia. While the industry represented by the respondents varies, the results and findings

may not be adequate to represent business organizations globally. In addition to that, the business culture and operating environment of New Zealand and Malaysia may not be generalizable to other jurisdictions that have similar intentions to adopt BDS. Future research work in this area may extend the generalizability of these research findings by testing the Sec-TOE framework for BDS adoption in multiple countries within multiple continents. Furthermore, the respondents of this research were limited to single key respondents of public-listed organizations in New Zealand and Malaysia. Therefore, this fact may also indicate that the results of this research may not be generalizable to other business sectors such as small-medium enterprises (SMEs). The single key respondent from each organization may also be indicative of that respondent's personal view and may not necessarily represent the actual view of the respondent's organization. Although single respondent from an organization is quite a common approach in organizational surveys, it would be beneficial for future work to have multiple respondents from different departments of an organization to gauge a better predictability of the measurement items/survey. Even though this research did not suffer from any response bias, having multiple respondents to represent one organization is expected to further strengthen the validity of research outcomes. One other limitation of the first phase survey is it does not allow the researcher to seek further clarification on any questions or concerns in order to gain further understanding of the received responses. Again, the researcher attempted to address this limitation by having a single case study to complement the findings of the survey (mixed-method approach).

With regards to the second phase of investigation namely the case study, limitations stem from the selection of a single case study. While the selected case was suitable due to it being a large banking institution, having traditionally worked with large volumes of data, and have started its own big data initiative, it still limits the generalizability of the findings. Despite this fact,

the researcher tried to derive meaning from the context of the selected case and reflected on how the findings may affect any theoretical generalizations. Thus, for future work, the suggestion is to conduct multiple case studies from various industries to allow for a comparison between cases, from various industries, and in turn identification of themes/findings that are more generalizable across industries. The single case study was conducted in Malaysia thus may not be able to fully complement the results of the first phase survey which was conducted in two countries. It is recommended for future work that employs the mixed-method approach to have study cases from the same countries as the respondents of the quantitative survey. This is to ensure a better representation of cases for triangulation purposes.

Future research work should also expand the research to look at the effect that the security determinants and constructs have on actual implementation of BDS, instead of only studying its effect on intention to adopt. New research work may also explore different techniques in data gathering for constructs testing in order to improve the measurements. Also, future work may further examine top management's view of security-related issues of BDS adoption, as their strategic decisions may influence security related investments needed for a BDS operating environment. Further work in security aspects and its relation to innovative technology adoption such as BDS will provide organizations with a better understanding on security issues. Thus, this understanding will allow them to make advance assessment and preparation of security plans and policies tailored to the requirements of the technology being adopted.

12. APPENDICES

The appendices are divided into two parts: 1) Appendices that are related to the first quantitative study, and 2) Appendices that are related to the second phase qualitative study. For the quantitative study, appendices included are the participants' information sheet (PIS), sample of an invitation note sent to participants, operationalization of constructs, the questionnaire, and loading and cross-loadings of indicator items. As for the second phase qualitative study, appendices included are the participants' information sheet, and the interview protocol. The PIS listed among others, the researcher's details, the research description and invitation to participate, and data storage information.

12.1 Appendices for First Phase Quantitative Study

The Department of Information Systems and Operation Management
The University of Auckland Business School
Level 4
Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand
+64 9 923 7154

The University of Auckland
Private Bag 92019
Auckland, New Zealand

PARTICIPANT INFORMATION SHEET (PIS)

Project title	:	Security Determinants in the Adoption of Big Data Solutions
Researcher	:	Khairulliza Ahmad Salleh
Degree	:	PhD in Information Systems

Department : Information Systems and Operations Management
Supervisor : Associate Professor Dr. Lech Janczewski *and*
Associate Professor Dr. Fernando Beltran

Researcher introduction
This research project is undertaken by Khairulliza Ahmad Salleh, a doctoral student in the Department of Information Systems and Operations Management (ISOM), Business School, The University of Auckland. The student is currently enrolled in a degree of PhD in Information Systems under the supervision of Associate Professor Dr. Lech Janczewski and co-supervised by Associate Professor Dr. Fernando Beltran.

Project description and invitation
Evolving trait of data being generated and stored has spurred the interest of organizations from various industries to adopt big data solutions (BDS) for solving specific business problems. However, as in any new technology adoption in organizations, BDS may also present security threats and challenges. Most threats are associated to the unique characteristics of big data, and the infrastructure that is required to support the size and scale of data collections. Thus, there should be a change in the way organizations manage and provide control towards its data. The process of adopting BDS should not only be seen as a technology adoption in increasing organizational efficiency, but instead, a more holistic manner should be prescribed in making adoption decision. Security aspects, besides from its technological and infrastructure need, should also be looked into from the organizational and environmental perspective. It has been agreed by security researchers that more research are needed to understand the interplay of organizational and environmental factors on information security issues.

Hence, the intent of this research is to examine the security determinants by focusing on the influence that various security technologies, organizational security view and security related environmental factors have on BDS adoption by organizations. The target respondent is organization's employee that is responsible for information security practices/policies in the organization OR those is knowledgeable about the organization's technology adoption practices (ONE respondent per organization).

For this purpose, the researcher would like to invite you to participate in this research. Your participation will be an important contribution to the successful outcome of this research.

Project procedures
This is a quantitative study, which uses an anonymous web-based (and paper) questionnaire as the method of data collection. The questionnaire will take about 10-15 minutes to complete. The questionnaire is available on a secure online survey website; **Qualtrics**. If you agree to participate in this research, please complete the web-based questionnaire at (**http://tinyurl.com/bdsadopt**). You may complete the questionnaire at any time convenient to you. You may also opt to answer the paper survey and return it to the researchers using the envelope provided. There is no expected physical, mental or social risks and harm associated with participation in this study. If you agree to participate in this research, please complete the web-based questionnaire at.

Your participation is voluntary in this research. Neither your position nor employment status with your organization will be affected by either your agreement or refusal to participate. No penalty or bonus will be given to those who participate or decline. For those who are interested in the findings, the researcher will be more than happy to provide you a summary of the findings after analysis have been finalized. Do contact the researchers using the contact details provided at the end of this PIS.

Data storage/retention/destruction/future use
The questionnaires will be stored in a secure, password-protected server or electronic storage devices at The University of Auckland and can only be accessed by the researcher and/or her supervisors. A backup copy will be stored on an external hard disk in a locked filing cabinet under the control of the researcher. These data will be stored for six (6) years, after which will be destroyed permanently by deleting the saved files from all storage, and hard copies will be cleared up by appropriate means of

incineration and destroyed by shredding. The findings of this study will be used for the researcher's doctoral thesis. They may also be included in published journal articles and conference proceedings.

Rights to Withdraw from Participation
This questionnaire has been approved by the University of Auckland's Human Participants Ethics Committee (UAHPEC). The questionnaire is done anonymously and you are under no obligation to participate in this research. If you do not wish to participate, you do not have to give a reason for this. Filling out and submitting the web-based questionnaire will indicate that you have given informed consent to participate. Please note that while you can withdraw from participation at any time, once you have submitted the web-based questionnaire, your data can no longer be withdrawn.

Anonymity and Confidentiality
All data will be used only for the purpose of this doctoral research and subsequent publications in academic journals. All data from participants will be aggregated during analysis and presented in a way that does not identify the source either by name and inference. Although some questions may be seen as sensitive, confidentiality of answers is guaranteed due to the anonymous nature of the questionnaire. It will not be possible to link a specific data to any individual participants thus ensuring anonymity. In addition, no personal identifiable information will be collected and IP address of respondents will not be recorded/saved. All results will appear in a generalize form.

Contact details
Should you have any queries or requiring any further details, below are the persons to be contacted:

Researcher: Khairulliza Ahmad Salleh
Email: k.salleh@auckland.ac.nz

Supervisor: Associate Professor Dr. Lech Janczewski
Phone: +64 9 923 7538
Email: l.janczewski@auckland.ac.nz

Co-Supervisor: Associate Professor Dr. Fernando Beltran
Phone: +64 9 923 7850
Email: f.beltran@auckland.ac.nz

Head of Department: Professor Michael D. Myers
Phone: +64 9 923 7468
Email: m.myers@auckland.ac.nz

For any concerns regarding ethical issues you may contact:

The Chair
The University of Auckland Human Participants Ethics Committee
The University of Auckland,
Research Office, Private Bag 92019,
Auckland, 1142.
Phone: +64 9 373 7599 ext. 83711
Email: ro-ethics@auckland.ac.nz

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE on 17 November 2015 for three years, Reference Number 016295.

The Department of Information Systems and Operation Management
The University of Auckland Business School
Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand
+64 9 923 7154

To whom it may concern,

SURVEY ON SECURITY DETERMINANTS IN THE ADOPTION OF BIG DATA SOLUTIONS IN ORGANIZATIONS

I am undertaking a doctoral research in the area of information systems security. The focus of my research is on security factors that acts as determinants in the adoption of big data solutions in organizations. By investigating the security determinants in BDS adoption, recommendation can be developed to address the factors that hinders adoption and leverage on the factors that may increase adoption.

I am writing to seek your support for your organization to participate in this research. The data will be collected in the form of an anonymous web-based questionnaire. I wish to assure you that all data obtained from this survey will be confidential and will be used only to provide support in fulfilling the objectives of this research.

Please find more information regarding this research on the enclosed Participant Information Sheet (PIS) and the Consent Form (CF). If you require clarification and any further information, please do not hesitate to contact me.

Thank you in anticipation of your valuable assistance.

Yours sincerely,
Khairulliza Ahmad Salleh
PhD Candidate
Department of Information Systems and Operations Management
The University of Auckland Business School
Auckland, New Zealand
Mobile No.: +64 21 082 70573
Email: k.salleh@auckland.ac.nz

OPERATIONALIZATION OF CONSTRUCTS

Independent Variables and Hypotheses

Variable	Definition	References	No of Items	Hypothesis (Relationship with BDS Adoption)
Technology Factors in Security				
Perceived Complexity	Degree of perceived complexity in ensuring security of BDS.	Borgman, Hans P., et al, 2013; Premkumar & Roberts, 1999	**3**	**-**
Perceived Compatibility	Degree of perceived compatibility of organizations' current security infrastructure with the security requirements of BDS.	Wang Yu Min et al., 2010; Ramamurthy et al., 1999	**3**	**+**
Organizational Factors in Security				
Top Management Support	Extent of top management support for IS security in BDS adoption.	Borgman, Hans P., et al, 2013; V. Grover, 1993; Knapp, Kenneth J., et al, 2006; Yap et al., 1992; A. Singh et al., 2014	**5**	**+**
Information Security Culture	Extent of information security culture existence in the organization.	Knapp, Kenneth J., et al, 2006; Williams et al. 2009; A. Singh et al., 2014	**6**	**+**
Organizational Learning Culture	Extent of organizational learning characteristics and orientation in the organization.	Baker and Sinkula, 1999	**6**	**+**
Environmental Factors in Security				

Security and Privacy Regulatory Concerns	Degree of concern in ensuring compliance to security and data privacy regulations in relation to BDS adoption.	Cumbley & Church, 2013; Tankard, 2012; Singh & Singh, 2012	**4**	-
Risks of Outsourcing	Perceived degree of security and privacy risks associated to outsourcing (outsource BDS or use of third-party tools).	Bachlechner et al, 2014; S. Sagiroglu, D. Sinanc, 2013; Hill and Liedtka, 2007	**5**	-

Dependent Variable and Measurement Item

Variable	Definition	References	No of Items
Intention to adopt Big Data Solution	Organizational intention to adopt BDS.	Teo et.al. (2003)	2

THE UNIVERSITY OF AUCKLAND
BUSINESS SCHOOL

A Survey on Security Determinants in the Adoption of Big Data Solutions in Organizations

This questionnaire is designed to evaluate information security management factors that affects the intention to adopt Big Data Solutions (BDS). The target respondents are organizations' Information Security personnel and/or those who are familiar with their organization's technology adoption processes. Please answer all questions accordingly.

Your responses to the questionnaire are kept confidential. The answers will be grouped together with the responses of other participants (aggregated) from other organizations, thus you cannot be identified individually.

It will take you about ten minutes to complete the questionnaire.

Would you like to receive a copy of the survey results?

☐ YES

☐ NO

If YES, please provide your email address: ……..

If you have any questions, contact the researchers at the following email address:

Email: k.salleh@auckland.ac.nz; l.janczewski@auckland.ac.nz

Department of Information Systems and Operations Management

The University of Auckland Business School

Owen G Glenn Building, 12 Grafton Road, Auckland, New Zealand

The University of Auckland, Private Bag 92019, Auckland, New Zealand

Telephone: 64 9 373 7599 Facsimile: 64 9 373 8797

SECTION A: PERSONAL BACKGROUND

TERMINOLOGY:

Big Data Solutions (BDS) is defined as a collection of technologies and framework that provides a platform to integrate, manage, and apply sophisticated computational processing to large data sets. The technologies and frameworks include Hadoop, MapReduce, NoSQL, Dyad, Apache Mahout, and other BDS from various technology provider. It may be used to support any organization wide or departmental function (customer analytics, risk analysis, experience analytics, sentiment analysis, product placing optimization, etc.).

Big Data refers to large data sets that may be analyzed computationally to reveal patterns, trends and associations. The most common forms of data analyzed in this way are business transactions stored in databases, followed by documents, e-mail, sensor data, clickstream data, and social media.

Instruction: Please answer the following questions by selecting the best option that describes yourself.

A1: Which job category best describes your job function in the organization?

	Chief Executive Officer (CEO) and/or President
	Chief Information Officer (CIO)/IT Director
	Chief Information Security Officer (CISO)
	IS/IT Management/Staff
	Info. Security Management/Staff
	Head of Business Unit/Department
	Others _____ (Please specify)

A2: Which of the following best describe your working experience?

	Less than 5 years
	5 – 10 years
	10 – 20 years
	More than 20 years

A3: Which of the following best describe your tenure in the current organization? (Please select one)

	Less than 5 years
	5 – 10 years
	10 – 20 years
	More than 20 years

SECTION B: ORGANIZATION BACKGROUND

Instruction: Please answer the following questions by selecting the best option that describes your organization.

B1: Which of the following best describe the industry of your organization?

	Construction and Real Estate
	Consumer Goods
	Education
	Energy and Natural Resources
	Financial Services
	Government/Public Sector
	Healthcare/Pharmaceuticals
	IT and Technology
	Manufacturing
	Professional Services
	Retail
	Telecommunication
	Others _____

B2: Which of the following best describe the number of employees in your organization?

	Less than 500
	501 to 1000
	1001 - 2000
	More than 2000

B3: In which country is the organization operating in (your current appointment)?

	New Zealand
	Malaysia

B4: Which of the following specific job functions exist within your organization? (Please select all that apply)

	Chief Information Officer/ IT Director
	Chief Information Security Officer
	Chief Risk Officer
	Information Security Management/Managers
	Information Security Staff

B5: How large is the IT/IS department in your organization?

	No IT/IS Department
	1-20 personnel
	21-100 personnel
	100-250 personnel
	More than 250 personnel
	Outsourced

B6: What is your organization's annual budget (approx.) for information technology/systems? (MYR/NZD)

	Less than 500k
	501k – 2M
	2.1M – 5M
	5.1M - 100M
	More than 100M
	Cannot be disclosed

B7: How large is your organization's Information Security (InfoSec) function?

	No InfoSec function
	1-5 personnel
	6-10 personnel
	11-20 personnel
	More than 20 personnel
	Outsourced

B8: What is the approximate amount of data processed by your organization?

	Above 100 terabytes/month
	1-100 terabytes/month
	500 gigabytes – 1 terabytes/month
	100 – 500 gigabytes/month
	Below 100 gigabytes/month
	Not aware of the amount

B9: Please select one category of BDS adoption that best reflects your organization's present status:

	Adopter
	Non-adopter

SECTION C: TECHNOLOGY, ORGANIZATIONAL, ENVIRONMENTAL SECURITY FACTORS

Instruction: The following questions relate to the moment when your organization first **CONSIDERED** to adopt Big Data Solutions (BDS) or for organizations without BDS, please answer according to the level of agreement that best reflects your organization's standpoint.

Please rate the following statements based on your knowledge of your organization's security practices (circle appropriate number in each row).

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
Establishing information security mechanisms for BDS is a complex process	1	2	3	4	5
The skills required to secure BDS are too complex for our employees	1	2	3	4	5
Integrating security requirement of BDS in our current work practices will be difficult	1	2	3	4	5
The changes introduced by BDS is compatible with the organization's existing information security practices	1	2	3	4	5
Security requirement of BDS is compatible with the organization's existing information security infrastructure	1	2	3	4	5
Development of information security mechanisms for BDS is compatible with the organization's existing experiences with similar systems.	1	2	3	4	5

Please rate the following statements based on your knowledge of your organization's practices (circle appropriate number in each row).

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
Top management supports the adoption of BDS	1	2	3	4	5
Top management accept possible risks which may result from adopting BDS	1	2	3	4	5
Top management takes information security issues into account when planning to adopt BDS	1	2	3	4	5
Top management allocate budget and manpower for information security functions	1	2	3	4	5
Top management has effectively communicated its support for information security goals in relation to BDS adoption	1	2	3	4	5

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
This organization creates a focus on security of organizational data among all employees	1	2	3	4	5
This organization makes sure that security of organizational data is the first thing on the mind of all employees	1	2	3	4	5
This organization makes organizational data security practices the key norm for all employees	1	2	3	4	5
This organization dedicates efforts to create organizational data security-focussed workforce	1	2	3	4	5
Employees of this organization value the importance of securing organizational data	1	2	3	4	5
Practicing good organizational data security measures is the accepted way of doing business in this organization	1	2	3	4	5
There is an agreement that the organization's security function's ability to learn is the key to information security effectiveness	1	2	3	4	5
The basic values of the security function in this organization include learning as key to improvement	1	2	3	4	5
The sense around the organization is that employee learning is an investment, not an expense	1	2	3	4	5
Learning is seen as a key commodity necessary to guarantee organizational survival	1	2	3	4	5
The collective wisdom in this organization is that once we quit learning, we endanger our future	1	2	3	4	5
The organization encourages its employees to pursue security certifications/accreditations	1	2	3	4	5

Please rate the following statements based on your knowledge of your organization's interaction with its operating environment (circle appropriate number in each row).

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
Adherence to security standards is a challenge with the collection, storage, analysis and reuse of big data	1	2	3	4	5
Compliance to privacy regulations is a challenge with the collection, storage, analysis and reuse of big data	1	2	3	4	5
It is harder to assess the compliance of all personal data collected by BDS with the requirements of data protection law	1	2	3	4	5
With the use of BDS, the organization is concern on legal implications due to non-compliance to privacy related regulations	1	2	3	4	5

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
Outsourcing BDS creates concerns on data security	1	2	3	4	5
Outsourcing BDS creates concerns on data privacy	1	2	3	4	5
Outsourcing BDS creates vulnerability in access control of the organization's information assets	1	2	3	4	5
Outsourcing BDS creates risks through excessive dependency towards vendor	1	2	3	4	5
Outsourcing BDS complicates corporate policy implementation in protecting this organization's information assets	1	2	3	4	5

Please rate the following statements based on your knowledge of your organization's intention in BDS adoption.

	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
This organization is contemplating adopting BDS	1	2	3	4	5
This organization has adopted or likely to adopt BDS within a year	1	2	3	4	5

SECTION D: ORGANIZATIONAL BIG DATA SECURITY CONCERNS

D1: On a scale from 1 to 10, how concerned would you be regarding security of big data solutions (BDS)? Please tick one of the boxes below (1 = Low to 10 = high).

1	2	3	4	5	6	7	8	9	10

D2: The CIA triad (Confidentiality, Integrity, and Availability) is the key principle often referred to when developing information security policies in organizations. From the perspective of any of the key security principles, please state your organization's main security concern in relation to BDS adoption.

Are you interested to take part in a case study (as interviewee) for the next phase of this research?

☐ YES

☐ NO

If YES, please provide your email address: ……..

THANK YOU FOR YOUR HELP

Please return the questionnaire in the envelope provided.

Approved by the University of Auckland Human Participants Ethics Committee on 17th November, 2015 for three years, Reference Number 016295.

LOADING AND CROSS LOADINGS OF INDICATOR ITEMS

	Perceived Compatibility	Perceived Complexity	InfoSec Culture	Learning Culture	Top Mgmt. Support	Outsourcing Risks	Regulatory Concern
PCM1	**0.878**	-0.445	0.512	0.454	0.503	-0.148	-0.324
PCM2	**0.873**	-0.455	0.498	0.452	0.439	-0.217	-0.256
PCM3	**0.861**	-0.448	0.496	0.472	0.426	-0.154	-0.307
PCX1	-0.421	**0.900**	-0.641	-0.454	-0.682	0.532	0.591
PCX2	-0.467	**0.891**	-0.619	-0.491	-0.716	0.514	0.523
PCX3	-0.495	**0.890**	-0.647	-0.381	-0.676	0.552	0.569
ISC1	0.514	-0.599	**0.828**	0.430	0.726	-0.323	-0.513
ISC2	0.510	-0.616	**0.881**	0.467	0.743	-0.391	-0.574
ISC3	0.457	-0.540	**0.821**	0.431	0.676	-0.381	-0.465
ISC4	0.464	-0.632	**0.886**	0.484	0.696	-0.349	-0.468
ISC5	0.457	-0.631	**0.840**	0.542	0.675	-0.388	-0.519
ISC6	0.486	-0.538	**0.747**	0.517	0.664	-0.317	-0.408
OLC3	0.404	-0.313	0.327	**0.589**	0.376	-0.160	-0.256
OLC4	0.400	-0.422	0.464	**0.769**	0.482	-0.266	-0.296
OLC5	0.394	-0.321	0.410	**0.756**	0.421	-0.109	-0.248
OLC6	0.391	-0.384	0.451	**0.787**	0.503	-0.182	-0.323
TMS1	0.555	-0.775	0.788	0.585	**0.940**	-0.419	-0.553
TMS2	0.349	-0.664	0.678	0.504	**0.838**	-0.352	-0.524
TMS3	0.436	-0.630	0.747	0.541	**0.888**	-0.431	-0.497
TMS4	0.447	-0.590	0.650	0.497	**0.820**	-0.382	-0.381
TMS5	0.506	-0.715	0.789	0.574	**0.893**	-0.415	-0.469
OR1	-0.111	0.477	-0.316	-0.184	-0.356	**0.865**	0.450
OR2	-0.237	0.566	-0.387	-0.286	-0.462	**0.881**	0.515
OR3	-0.159	0.520	-0.414	-0.177	-0.376	**0.891**	0.529
RC1	-0.309	0.485	-0.523	-0.306	-0.452	0.400	**0.802**
Rc2	-0.285	0.452	-0.417	-0.239	-0.357	0.455	**0.837**
RC3	-0.303	0.584	-0.559	-0.413	-0.558	0.529	**0.858**
RC4	-0.245	0.565	-0.469	-0.323	-0.481	0.517	**0.848**

12.2 Appendices for Second Phase Qualitative Study

The Department of Information Systems and Operation Management
The University of Auckland Business School
Level 4
Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand
+64 9 923 7154

The University of Auckland
Private Bag 92019
Auckland, New Zealand

PARTICIPANT INFORMATION SHEET (PIS)

Project title	:	Security Determinants in the Adoption of Big Data Solutions
Researcher	:	Khairulliza Ahmad Salleh
Degree	:	PhD in Information Systems
Department	:	Information Systems and Operations Management
Supervisor	:	Associate Professor Dr. Lech Janczewski *and* Associate Professor Dr. Fernando Beltran

Researcher introduction

This research project is undertaken by Khairulliza Ahmad Salleh, a doctoral student in the Department of Information Systems and Operations Management (ISOM), Business School, The University of Auckland. The student is currently enrolled in a degree of PhD in Information Systems under the supervision of Associate Professor Dr. Lech Janczewski and co-supervised by Associate Professor Dr. Fernando Beltran.

Project description and invitation

Evolving trait of data being generated and stored has spurred the interest of organizations from various industries to adopt big data solutions (BDS) for solving specific business problems. However, as in any new technology adoption in organizations, BDS may also present security threats and challenges. Most threats are associated to the unique characteristics of big data, and the infrastructure that is required to support the size and scale of data collections. Thus, a change is expected in the way organizations manage and provide control towards its data. The process of adopting BDS should not only be seen as a technology adoption in increasing organizational efficiency, but instead, a more holistic manner should be prescribed in making adoption decision. Security aspects, besides from its technological and

infrastructure need, should also be looked into from the organizational and environmental perspective. It has been agreed by security researchers that more research are needed to understand the interplay of organizational and environmental factors on information security issues.

Hence, the intent of this research is to examine the security determinants by focusing on the influence that various security technologies, organizational security view and security related environmental factors have on BDS adoption by organizations. The target respondents are organization's employees that are responsible for information security practices/policies in the organization OR those who are knowledgeable about the organization's technology adoption practices. Other employees who are direct users of the big data solutions or receivers of data generated by the solutions may also be the respondents.

For this purpose, the researcher would like to invite you to participate in this research. Your participation will be an important contribution to the successful outcome of this research.

Project procedures
This is a case study, which uses semi-structured interview as the method of data collection. The semi-structured interview involves the use of some pre-formulated questions but some new questions may emerge during the conversation. Each interview should not require more than 1 hour to complete. There is no expected physical, mental or social risks and harm associated with participation in this study.

Your participation is voluntary in this research. Neither your position nor employment status with your organization will be affected by either your agreement or refusal to participate. No penalty or bonus will be given to those who participate or decline. For those who are interested in the findings, the researcher will be more than happy to provide you a summary of the findings after analysis have been finalized. Do contact the researchers using the contact details provided at the end of this PIS.

Data storage/retention/destruction/future use
The recording of the interview together with the transcribed version of it will be stored in a secure, password-protected server or electronic storage devices at The University of Auckland and can only be accessed by the researcher and/or her supervisors. A backup copy will be stored on an external hard disk in a locked filing cabinet under the control of the researcher. These data will be stored for six (6) years, after which will be destroyed permanently by deleting the saved files from all storage, and hard copies will be cleared up by appropriate means of incineration and destroyed by shredding. The findings of this study will be used for the researcher's doctoral thesis. They may also be included in published journal articles and conference proceedings.

Rights to Withdraw from Participation
This research has been approved by the University of Auckland's Human Participants Ethics Committee (UAHPEC). The researcher will audio-record the interview, however, participant may ask to stop the recording at any point during the interview. In addition, the participant may choose to stop participating at any time during the interview and may choose to withdraw their data at any time up to two weeks after the interview.

Anonymity and Confidentiality
All data will be used only for the purpose of this doctoral research and subsequent publications in academic journals. All data will be de-identified during analysis and presented in a way that does not identify the source. Although some questions may be seen as sensitive, confidentiality of answers is guaranteed. It will not be possible to link a specific data to any individual participants thus ensuring anonymity. All results will appear in a generalize form.

Contact details
Should you have any queries or requiring any further details, below are the persons to be contacted:

Researcher: Khairulliza Ahmad Salleh

Email: k.salleh@auckland.ac.nz
Supervisor: Associate Professor Dr. Lech Janczewski
Phone: +64 9 923 7538
Email: l.janczewski@auckland.ac.nz

Co-Supervisor: Associate Professor Dr. Fernando Beltran
Phone: +64 9 923 7850
Email: f.beltran@auckland.ac.nz

Head of Department: Professor Michael D. Myers
Phone: +64 9 923 7468
Email: m.myers@auckland.ac.nz

For any concerns regarding ethical issues you may contact:

The Chair
The University of Auckland Human Participants Ethics Committee
The University of Auckland,
Research Office, Private Bag 92019,
Auckland, 1142.
Phone: +64 9 373 7599 ext. 83711
Email: ro-ethics@auckland.ac.nz

Approved by the University of Auckland Human Participants Ethics Committee on 17 November 2015 for three years, Reference Number 016295.

The Department of Information Systems and Operation Management
The University of Auckland Business School
Level 4
Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand
+64 9 923 7154

INTERVIEW PROTOCOL

THIS FORM WILL BE HELD FOR A PERIOD OF SIX (6) YEARS

Project title	:	Security Determinants in the Adoption of Big Data Solutions
Researcher	:	Khairulliza Ahmad Salleh
Degree	:	PhD in Information Systems
Supervisor	:	Associate Professor Dr. Lech Janczewski *and* Associate Professor Dr. Fernando Beltran

Please note that in a semi-structured interview, data gathering tends to be open-ended. Data gathered from one interview session could suggest directions to purse in subsequent interview sessions. Therefore, it is not possible to present a complete inventory of all the questions that might be asked in the interviews. However, all questions are structured around the following categories: 1) technological, organizational and environmental factors affecting the adoption of Big Data Solutions (BDS) 2) the main information security changes introduced by adopting BDS (pre and post BDS); and 3) the main challenges in managing big data from security view.

The following questions give you an idea of the issues that will be explored. It is important to note that all these questions are going to be conversed from an information security perspective.

1) How does this organization keep abreast of developments that may affect its security requirements? With BDS, does this organization view any changes in security requirements?
2) How does the complexity of securing BDS affect the BDS adoption decision?

3) What is the organization's view on the compatibility of existing security mechanisms deployed in the organization with the ones required by BDS? Will compatibility positively affect adoption decision?
4) How are recommendations to adopt BDS brought forward? What is the communication process? Does security aspects play any role in the adoption process?
5) Is top management support important in adoption decision? Is the support for security functions communicated efficiently by the top management?
6) What influence do learning activities have in monitoring potential, new, or existing security vulnerabilities or threats?
7) How would you characterize the level of security awareness across the organization? How does security awareness help in avoiding data and information breach?
8) What effect does privacy regulations have on your organization's BDS adoption process? Is there any other environmental factors (factors from outside the organization) affecting the adoption process?
9) Big data is characteristically large in volume and derived from various sources. How does this organization determine the level of security appropriate for adequately protecting all information resources? Is there any difference in security mechanisms deployed (differ from pre and post adoption)?
10) What do you believe to be important security considerations when evaluating BDS for adoption?
11) How do technological attributes of BDS differ from the attributes considered important for other information technologies? Do you notice any attributes unique to BDS?
12) What is the organizational view on the main challenges in managing big data security? In the CIA triad (Confidentiality, Integrity, Availability), which factor is considered the most difficult to attain with the use of BDS?

Approved by the University of Auckland Human Participants Ethics Committee on 17 November 2015 for three years, Reference Number 016295.

References

Abbasi, A., Sarker, S., & Chiang, R. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Journal of the Association for Information Systems*, *17*(2), i–xxxii.

Abdullah, M. F., Ibrahim, M., & Zulkifli, H. (2017). Big data analytics framework for natural disaster management in Malaysia. *IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, (IoTBDS), 406–411. https://doi.org/10.5220/0006367204060411

Agarwal, R., & Prasad, J. (1998). The antecedents and consequents of user perceptions in information technology adoption. *Decision Support Systems*, *22*(1), 15–29. https://doi.org/10.1016/S0167-9236(97)00006-7

Ahmad Salleh, K., & Janczewski, L. (2018). An Implementation of Sec-TOE Framework : Identifying Security Determinants of Big Data Solutions Adoption. *PACIS 2018 Proceedings*, 211.

Ahmad Salleh, K., & Janczewski, L. (2019). *Security Considerations in Big Data Solutions Adoption: Lessons from a Case Study on a Banking Institution*. Procedia Computer Science,164,168-176.

Ahmad Salleh, K., Janczewski, L., & Beltran, F. (2015). SEC-TOE Framework : Exploring Security Determinants in Big Data Solutions Adoption. *PACIS 2015 Proceedings. Paper 203*. Retrieved from http://aisel.aisnet.org/pacis2015/203

Al-qirim, N., Tarhini, A., & Rouibah, K. (2017). Determinants of Big Data Adoption and Success. *Proceedings of the International Conference on Algorithms, Computing and Systems*, 88–92.

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alturki, U., Alamri, M. M., Saud, M. S. Bin, Alhamed, O. A. (2019). Big Data Adoption and Knowledge Management Sharing: An Empirical Investigation on their Adoption and Sustainability as a Purpose of Education. *IEEE Access*, *7*, 1–1. https://doi.org/10.1109/ACCESS.2019.2906668

Al-sai, Z. A., Abdullah, R., & Husin, M. H. (2019). Big Data Impacts and Challenges : A Review. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 150–155. IEEE.

Alley-young, G. (2017). White House Big Data Initiative. *Encyclopedia of Big Data*, 1–5. https://doi.org/10.1007/978-3-319-32001-4

Alshboul, Y., & Wang, YongNepali, R. K. (2015). Big Data LifeCycle : Threats and Security Model. *Twenty-First Americas Conference on Information Systems*, 1–7.

Ananthalakshmi, A., & Bergin, T. (2018). Malaysian central bank says foiled attempted cyber-heist. *Reuters*. Retrieved from https://www.reuters.com/article/us-malaysia-cenbank-cybersecurity-incide/malaysian-central-bank-says-foiled-attempted-cyber-heist-idUSKBN1H50YF

Arfat, Y., Usman, S., Mehmood, R., & Katib, I. (2020). Big Data Tools, Technologies, and Applications: A Survey. In R. Mehmood, S. See, I. Katib, & I. Chlamtac (Eds.), *Smart Infrastructure and Applications* (pp. 453–490). https://doi.org/10.1007/978-3-030-13705-2_19

Ashabi, A., Sahibuddin, S. Bin, & Haghighi, M. S. (2020). Big Data: Current Challenges and Future Scope. *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 131–134. https://doi.org/10.1109/iscaie47305.2020.9108826

Asian Institute of Chartered Bankers, PWC. (2018). *Building a Cyber Resilient Financial Instutitions: Are You Ready for the Imminent Breach?* Retrieved from *https://www.pwc.com/my/en/assets/publications/2018/aicb-pwc-publication.pdf*

Baig, M. I., Shuib, L., & Yadegaridehkordi, E. (2019). Big data adoption: State of the art and

research challenges. *Information Processing and Management*, *56*(6). https://doi.org/10.1016/j.ipm.2019.102095

Baker, J. (2011). The Technology–Organization– Environment Framework. In *Information Systems Theory: Explaining and Predicting our Digital Society Vol. 1* (pp. 231–245). https://doi.org/10.1007/978-1-4419-6108-2

Baker, J. (2012). Information Systems Theory. *Information Systems Theory: Explaining and Predicting Our Digital Society*, *1*, 231–245. https://doi.org/10.1007/978-1-4419-6108-2

Balachandran, B. M., & Prasad, S. (2017). Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence. *Procedia Computer Science*, *112*, 1112–1122. https://doi.org/10.1016/j.procs.2017.08.138

Bansal, A., Kaur, A., & Aggarwal, A. (2014). Big data explosion: insight for new age managers. *International Journal Of Scientific & Enegineering Research*, *5*(5), 7–11.

Barbosa, M. W., Vicente, A. de la C., Ladeira, M. B., & de Oliveira, M. P. V. (2018). Managing supply chain resources with Big Data Analytics: a systematic review. *International Journal of Logistics Research and Applications*, *21*(3), 177–200. https://doi.org/10.1080/13675567.2017.1369501

Barclay, D., Higgins, C., & Hompson, R. (1995). The Partial Least Squares (PLS) Approach to Causal Modelling: Personal Computer Adoption and Use as an Illustration. *Technology Studies, Special Issue on Research Methodology*, *2*(2), 285–309.

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of things: A survey of technologies and security risks in smart home and city environments. *IET Conference Publications*, *2018*(CP740). https://doi.org/10.1049/cp.2018.0030

Bedeley, R., & Iyer, L. S. (2014). Big Data Opportunities and Challenges: the Case of Banking Industry. *SAIS 2014 Proceedings*, 7. Retrieved from http://aisel.aisnet.org/sais2014/2/

Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In *Information Systems Outsourcing* (pp. 313–334). https://doi.org/10.1007/978-3-030-45819-5_13

Benjelloun, F.-Z., & Lahcen, A. A. (2015). Big Data Security: Challenges, Recommendations and Solutions. In *Web Services: Concepts, Methodologies, Tools, and Applications* (pp. 301–313). https://doi.org/10.4018/978-1-5225-7501-6.ch003

Bertino, E., & Ferrari, E. (2018). Big Data Security and Privacy. In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years* (Vol. 31, pp. 425–439). https://doi.org/10.1007/978-3-319-61893-7

Bhimani, A. (2015). Exploring big data's strategic consequences. *Journal of Information Technology*, *30*(1), 66–69. https://doi.org/10.1057/jit.2014.29

Big Data Working Group. (2013). *Expanded Top Ten Big Data Security and Privacy Challenges*. Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. *2013 46th Hawaii International Conference on System Sciences*, 4425–4435. https://doi.org/10.1109/HICSS.2013.132

Boyatzis, R. (1998). Thematic analysis and code development: Transforming qualitative information. In *London and New Delhi: Sage Publications*. https://doi.org/10.1177/102831539700100211

Bremser, C. (2018). Starting Points for Big Data Adoption. *Twenty-Sixth European Conference on Information Systems (ECIS2018)*. Retrieved from http://ecis2018.eu/wp-content/uploads/2018/09/1228-doc.pdf

Buhl, H. U., & Heidemann, J. (2013). Big Data A Fashionable Topic with (out) Sustainable

Relevance for Research and Practice ? *Business and Information Systems Engineering*, *5*(2), 66–69. https://doi.org/10.1007/s12599-013-0249-5

Cabrera-Sanchez, J.-P., & Villarejo-Ramos, A. F. (2019). Factors Affecting The Adoption Of Big Data Analytics In Companies. *RAE Journal of Business Management*, *59*(December), 415–429.

Chakravarthi, M. A., & Srinivas, O. (2017). The etymology of big data on government processes. *2017 International Conference on Information Communication and Embedded Systems, ICICES 2017*. https://doi.org/10.1109/ICICES.2017.8070712

Chang, R. M., Kauffman, R. J., & Kwon, Y. (2014). Understanding the paradigm shift to computational social science in the presence of big data. *Decision Support Systems*, *63*, 67–80. https://doi.org/10.1016/j.dss.2013.08.008

Chang, V. (2015). Towards a Big Data system disaster recovery in a Private Cloud. *Ad Hoc Networks*, *000*, 1–18. https://doi.org/10.1016/j.adhoc.2015.07.012

Chau, P. Y. K., & Tam, K. Y. (1997). Factors Affecting the Adoption of Open Systems : An Exploratory. *MIS Quarterly*, *21*(1), 1–24.

Chen, H., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big DAta to Big Impact. *MIS Quarterly*, *36*(4), 1165–1188.

Chen, J., Liang, Q., & Wang, J. (2015). Secure transmission for big data based on nested sampling and coprime sampling with spectrum efficiency. *Security and Communication Networks*, *8*(14), 2448–2456. https://doi.org/10.1002/sec

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171–209. https://doi.org/10.1007/s11036-013-0489-0

Chen, Y., Chen, H., Gorkhali, A., Lu, Y., Ma, Y., & Li, L. (2016). Big data analytics and big data science: a survey. *Journal of Management Analytics*, *3*(1), 1–42. https://doi.org/10.1080/23270012.2016.1141332

Chenthara, S., Wang, H., & Ahmed, K. (2018). Security and privacy challenges in big data environment. In S. Sakr & A. Zomaya (Eds.), *Encyclopedia of Big Data Technologies* (pp. 1–9).

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, *16*(5), 484–501.

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Clarke, R. (2016). Big data, big risks. *Information Systems Journal*, *26*(1), 77–90. https://doi.org/10.1111/isj.12088

Cohen, D., Gan, C., Hwa, H. A. Y., & Chong, E. (2007). Customer Retention by Banks in New Zealand. *Banks and Bank Systems*, *2*(1), 40–55.

Cohen, J. (2013). Statistical power analysis for the behavioral sciences. In *Statistical Power Analysis for the Behavioral Sciences* (Vol. 2nd). https://doi.org/10.1234/12345678

Compeau, D., & Higgins, C. A. (1995). Computer Self-Efficacy:Development of a Measure and Initial Test. *MIS Quarterly*, (June), 189–212.

Costa, C., & Santos, M. Y. (2017). Big Data: State-of-the-art concepts, techniques, technologies, modeling approaches and research challenges. *IAENG International Journal of Computer Science*, *44*(3), 285–301.

Creswell, J. W., & Clark, V. L. P. (2011). Designing and conducting mixed methods research. In *Designing and conducting mixed methods research.* (2nd Edition). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2006-11884-000&site=ehost-live&scope=site

Creswell, J. W., & Clark, V. L. P. (2018). *Designing and Conducting Mixed Methods Research*

(3rd Editio). Sage Publications.
Cruz-Jesus, F., Pinheiro, A., & Oliveira, T. (2019). Understanding CRM adoption stages: empirical analysis building on the TOE framework. *Computers in Industry*, *109*, 1–13. https://doi.org/10.1016/j.compind.2019.03.007
Cumbley, R., & Church, P. (2013). Is "Big Data" creepy? *Computer Law & Security Review*, *29*(5), 601–609. https://doi.org/10.1016/j.clsr.2013.07.007
Da Veiga, a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
Da Veiga, A., Martins, N., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *South African Business Review*, *11*(1), 147–166.
Davenport, T. H. (2014). *Big Data at Work: Dispelling the Myths, Uncovering the Opportunities*. Massachusetts: Harvard Business School Publishing Corporation.
Davenport, T. H., & Dyche, J. (2013). *Big Data in Big Companies*. Retrieved from https://www.iqpc.com/media/7863/11710.pdf
Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.
Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982
De Villiers, M. R. (2012). Models for interpretive information systems research, part 1: Is research, action research, grounded theory - a meta-study and examples. In M. Mora, O. Gelman, A. Steenkemp, & M. S. Raisinghani (Eds.), *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems* (pp. 222–237). https://doi.org/10.4018/978-1-4666-0179-6.ch011
Demchenko, Y., Ngo, C., Laat, C. De, & Membrey, P. (2014). Big Security for Big Data: Addressing Security Challenges for the Big Data Infrastructure. In W. Jonker & M. Petković (Eds.), *Secure Data Management* (pp. 76–94). https://doi.org/10.1007/978-3-319-06811-4
DePietro, R., Wiarda, E., & Fleischer, M. (1990). The Context for Change: Organization, Technology and Environment. In L. G. Tornatzky & M. Fleischer (Eds.), *The Processes of Technological Innovation* (pp. 151–175).
Desanctis, G., & Courtney, J. F. (1983). Toward Friendly User MIS Implementation. *Communications of the ACM*, *26*(10), 732–738.
Dev Mishra, A., & Beer Singh, Y. (2017). Big data analytics for security and privacy challenges. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 50–53. https://doi.org/10.1109/CCAA.2016.7813688
Dhar, S., & Mazumdar, S. (2014). Challenges and best practices for enterprise adoption of Big Data technologies. *2014 IEEE International Technology Management Conference, ITMC 2014*. https://doi.org/10.1109/ITMC.2014.6918592
Dhillon, G. (1997). *Managing Information System Security*. Houndmills, Basingstoke, Hampshire: MacMillan Press Ltd.
Dhillon, G., Syed, R., & Sá-Soares, F. de. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information and Management*, *54*(4), 452–464. https://doi.org/10.1016/j.im.2016.10.002
Dollah, R., & Aris, H. (2018). A review of sector-specific big data analytics models. *2017 IEEE Conference on Big Data and Analytics, ICBDA 2017*, *2018-Janua*, 72–80. https://doi.org/10.1109/ICBDAA.2017.8284110
Dong, X., Li, R., He, H., Zhou, W., Xue, Z., & Wu, H. (2015). Secure sensitive data sharing on a big data platform. *Tsinghua Science and Technology*, *20*(1), 72–80.

https://doi.org/10.1109/TST.2015.7040516
Dresner Advisory Services. (2017). *Big Data Analytics Market Study - 2017 edition*. Retrieved from https://www.microstrategy.com/getmedia/cd052225-be60-49fd-ab1c-4984ebc3cde9/Dresner-Report-Big_Data_Analytic_Market_Study-WisdomofCrowdsSeries-2017
Duncan, B., Whittington, M., & Chang, V. (2018). Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, *2018-Janua*(August), 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308189
Dzazali, S. (2014). Public Sector Big Data Analytics Initiative : Malaysia's Perspective. Retrieved from MAMPU website: http://www.mampu.gov.my/documents/10228/1242104/1.+KEYNOTE+MAMPU.pdf/cd0b9e10-a999-42d8-bd54-8f44a1b12b5b
Eckhoff, D., & Sommer, C. (2014). Driving for Big Data? Privacy Concerns in Vehicular Networking. *IEEE Security & Privacy*, *12*(1), 77–79. https://doi.org/10.1109/MSP.2014.2
Ekbia, H., Bowman, T., & Weingart, S. (2015). Big Data , Bigger Dilemmas : A Critical Review. *Journal of the Association for Information Science and Technology*, *66*(8), 1523–1545. https://doi.org/10.1002/asi
Fang, H., Zhang, Z., Wang, C. J., & Daneshmand, M. (2015). A survey of big data research. *IEEE Network*, *29*(5), 6. https://doi.org/10.1109/MNET.2015.7293298
Feilzer, M. Y. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research*, *4*(1), 6–16. https://doi.org/10.1177/1558689809349691
Fichman, R. G., & Kemerer, C. F. (1997). The Assimilation Of Software Process Innovations: An Organizational Learning Perspective. *Management Science*, *43*(10), 1345–1363.
Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research. In *Reading MA AddisonWesley*. Retrieved from http://people.umass.edu/aizen/f&a1975.html
Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382. https://doi.org/10.2307/3150980
Frické, M. (2015). Big Data and Its Epistemology. *Journal of the Association for Information Science and Technology*, *66*(4), 651–661. https://doi.org/10.1002/asi
Frizzo-Barker, J., Chow-White, P. A., Mozafari, M., & Ha, D. (2016). An empirical study of the rise of big data in business scholarship. *International Journal of Information Management*, *36*(3), 403–413. https://doi.org/10.1016/j.ijinfomgt.2016.01.006
Gartner (2012). *Market Trends: Big Data Opportunities in Vertical Industries*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2012/08/16/roundup-of-big-data-forecasts-and-market-estimates-2012/
Gartner (2012). *The Importance of ' Big Data ': A Definition*. Retrieved from http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=2057415&ref=QuickSearch&sthkw=the+importance+of+%27big+data%27%3AA+definition
Gartner Inc. (2014). *Survey Analysis : Big Data Investment Grows but Deployments Remain Scarce in 2014*. Retrieved from https://www.gartner.com/en/documents/2841519/survey-analysis-big-data-investment-grows-but-deployment
Ghani, K. R., Zheng, K., Wei, J. T., & Friedman, C. P. (2014). Harnessing Big Data for Health Care and Research: Are Urologists Ready? *European Urology*. https://doi.org/10.1016/j.eururo.2014.07.032
Göb, R. (2014). Discussion of "Reliability Meets Big Data: Opportunities and Challenges."

Quality Engineering, *26*(1), 121–126. https://doi.org/10.1080/08982112.2014.846124
Goes, P. B. (2014). Editor's Comments: Big Data and IS Research. *MIS Quarterly*, *38*(3).
Goodendorf, L. (2013). Managing Big Data Security Concerns. *Information Security*, March, 29–33.
Goodhue, D., & Thompson, R. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, *19*(2), 213–236.
Grover, V. (1993). An Empirically Derived Model for the Adoption of Customer-based Interorganizational Systems. *Decision Sciences*, *24*(3), 603–640. https://doi.org/10.1111/j.1540-5915.1993.tb01295.x
Gupta, N. K., & Rohil, M. K. (2020). Big Data Security Challenges and Preventive Solutions. In Neha Sharma, A. Chakrabarti, & V. E. Balas (Eds.), *Data Management, Analytics and Innovation* (Vol. 1, pp. 285–299). https://doi.org/10.1007/978-981-32-9949-8_21
Gurrin, C., & Smeaton, A. F. (2014). LifeLogging : Personal Big Data. *Foundations and Trends in Information Retrieval*, *8*(1), 1–107. https://doi.org/10.1561/1500000033
Haeussinger, F., & Kranz, J. (2017). Antecedents of Employees ' Information Security Awareness - Review , Synthesis , and Directions for Future Research. *Proceedings of the 25th European Conference on Information Systems (ECIS)*.
Hair, F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202
Hair, F, Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). Multivariate Data Analysis. *Prentice Hall*, Upper Saddle River, NJ: Prentice Hall
Hashem, I. A. T., Yaqoob, I., Badrul Anuar, N., Mokhtar, S., Gani, A., & Ullah Khan, S. (2014). The rise of "Big Data" on cloud computing: Review and open research issues. *Information Systems*, *47*, 98–115. https://doi.org/10.1016/j.is.2014.07.006
Hayashi, K. (2013). Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility. *2013 International Conference on Availability, Reliability and Security*, 506–511. https://doi.org/10.1109/ARES.2013.66
Herath, T. C., Herath, H. S. B., & D'Arcy, J. (2020). Organizational Adoption of Information Security Solutions: An Integrative Lens Based on Innovation Adoption and the Technology-Organization-Environment Framework. *Data Base for Advances in Information Systems*, *51*(2), 12–35. https://doi.org/10.1145/3400043.3400046
Hofmann, E. (2017). Big data and supply chain decisions: the impact of volume, variety and velocity properties on the bullwhip effect. *International Journal of Production Research*, *55*(17), 5108–5126. https://doi.org/10.1080/00207543.2015.1061222
Hota, C., Upadhyaya, S., & Al-Karaki, J. N. (2015). Advances in secure knowledge management in the big data era. *Information Systems Frontiers*, *17*(5), 983–986. https://doi.org/10.1007/s10796-015-9593-y
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x
Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Managament Journal*, *20*(2), 195–204.
IDC. (2013). *New IDC Worldwide Big Data Technology and Services Forecast Shows Market Expected to Grow to $32 billion in 2007*. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS24542113
IDC. (2015). *Asia / Pacific Big Data Technology and Services 2014 – 2018 Analysis and Forecast*.
IDC. (2019). *The Changing Face of Data Security: 2019 Thales Data Threat Report, Global*

Edition. Retrieved from https://go.thalesesecurity.com/rs/480-LWA-970/images/2019-DTR-Global-A4-Web-ar.pdf

IDG Enterprise. (2014). *Big Data: A Survey* (Vol. 19). https://doi.org/10.1007/s11036-013-0489-0

IDG Enterprise. (2015). *2015 Big Data and Analytics Survey*. https://doi.org/10.1007/978-3-319-10665-6

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Field Methods*, *18*(1), 3–20. https://doi.org/10.1177/1525822X05282260

Jagadish, H. V., Gehrke, J., Labrinidis, A., Papakonstantinou, Y., Patel, J. M., Ramakrishnan, R., & Shahabi, C. (2014). Big data and its technical challenges. *Communications of the ACM*, *57*(7), 86–94. https://doi.org/10.1145/2611567

Jain, P., Gyanchandani, M., & Khare, N. (2019). Enhanced Secured Map Reduce layer for Big Data privacy and security. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0193-4

Jarke, M. (2013). Interview with Stefan Wrobel on " Applied Big Data Research ." *Business and Information Systems Engineering*, *6*(5), 303–304. https://doi.org/10.1007/s12599-014-0336-2

Jeong, S. R., & Ghani, I. (2014). Semantic Computing for Big Data : Approaches , Tools , and Emerging Directions. *KSII Transactions on Internet and Information Systems*, *8*(6), 2022–2042.

Johri, P., Arora, S., & Kumar, M. (2018). Privacy Preserve Hadoop (PPH)—An Implementation of BIG DATA Security by Hadoop with Encrypted HDFS. *Lecture Notes in Networks and Systems*, *10*, 339–346. https://doi.org/10.1007/978-981-10-3920-1_35

Johri, P., Kumar, A., Das, S., & Arora, S. (2017). Security framework using Hadoop for big data. *Computing, Communication and Automation (ICCCA), 2017 International Conference On*, 268–272.

Hair, F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage Publications.

Kaisler, S., Armour, F., Espinosa, J. a, & Money, W. (2013). Big Data: Issues and Challenges Moving Forward. *46th Hawaii International Conference on System Sciences (HICSS)*, 995–1004. https://doi.org/10.1109/HICSS.2013.645

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kataria, M., & Mittal, M. P. (2014). Big Data : A Review. *International Journal of Computer Science and Mobile Computing*, *3*(7), 106–110.

Kemelor, P. (2015). Digital Data Grows into Big Data. *IT Professional*, *17*(4), 42–48. https://doi.org/10.1109/MITP.2015.69

Kemp, R. (2014). Legal aspects of managing Big Data. *Computer Law and Security Review*, *30*(5), 482–491. https://doi.org/10.1016/j.clsr.2014.07.006

Khidzir, N. Z., Mohamed, A., & Arshad, N. H. (2010). Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. *2010 International Conference on Information Retrieval & Knowledge Management (CAMP)*, 194–199. https://doi.org/10.1109/INFRKM.2010.5466918

Kim, G.-H., Trimi, S., & Chung, J.-H. (2014). Big-data applications in the government sector. *Communications of the ACM*, *57*(3), 78–85. https://doi.org/10.1145/2500873

Klassen, A. C., Creswell, J., Plano Clark, V. L., Smith, K. C., & Meissner, H. I. (2012). Best practices in mixed methods for quality of life research. *Quality of Life Research*, *21*(3), 377–380. https://doi.org/10.1007/s11136-012-0122-x

Klievink, B., Romijn, B. J., Cunningham, S., & de Bruijn, H. (2017). Big data in the public sector: Uncertainties and readiness. *Information Systems Frontiers*, *19*(2), 267–283. https://doi.org/10.1007/s10796-016-9686-2

Knapp, J., Marshall, T. E., Rainer, J., & Morrow, D. W. (2004). *Top Ranked Information Security Issues : Certification Consortium (ISC) 2 Survey Results*. Auburn, Alabama.

Knapp, J, Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer*, *14*(1), 24–36.

Kourid, A., Chikhi, S., & Hong, S. (2017). A comparative study of recent advances in Big data Security and Privacy. *Asia-Pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, *7*(5), 873–883. https://doi.org/10.14257/ajmahs.2017.05.23

Kshetri, N. (2014). Big data′s impact on privacy, security and consumer welfare. *Telecommunications Policy*, 1–12. https://doi.org/10.1016/j.telpol.2014.10.002

Kwon, O., Lee, N., & Shin, B. (2014). Data quality management, data usage experience and acquisition intention of big data analytics. *International Journal of Information Management*, *34*(3), 387–394. https://doi.org/10.1016/j.ijinfomgt.2014.02.002

Kwon, T. H., & Zmud, R. W. (1987). Unifying the fragmented models of information systems implementation. In *Critical issues in information systems research* (pp. 227–251). Retrieved from http://portal.acm.org/citation.cfm?id=54905.54915

Lafuente, G. (2015). The big data security challenge. *Network Security*, *2015*(1), 12–14. https://doi.org/10.1016/S1353-4858(15)70009-7Feature

Lai, Y., Sun, H., & Ren, J. (2018). Understanding the determinants of big data analytics (BDA) adoption in logistics and supply chain management: An empirical investigation. *International Journal of Logistics Management*, *29*(2), 676–703. https://doi.org/10.1108/IJLM-06-2017-0153

Lane, A. (2014). In Defense of Big Data. *Information Security*, (August), 4–11.

Laney, D. (2001). *3D Data Management: Controlling Data Volume, Velocity, and Variety*. Retrieved from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Latif, Z., Lei, W., Latif, S., Pathan, Z. H., Ullah, R., & Jianqiu, Z. (2019). Big data challenges: Prioritizing by decision-making process using Analytic Network Process technique. *Multimedia Tools and Applications*, *78*(19), 27127–27153. https://doi.org/10.1007/s11042-017-5161-4

Lee, I. (2017a). Big data: Dimensions, evolution, impacts, and challenges. *Business Horizons*, *60*(3), 293–303. https://doi.org/10.1016/j.bushor.2017.01.004

Li, H., Wu, J., Liu, L., & Li, Q. (2015). *Adoption of Big Data Analytics in Healthcare : The Efficiency and Privacy*. PACIS 2015 Proceedings. 181.

Li, S., & Gao, J. (2016). Security and Privacy for Big Data. In S. Yu & S. Guo (Eds.), *Big Data Concepts, Theories and Applications* (pp. 281–313). https://doi.org/10.1007/978-3-319-27763-9

Lim, J. S., Ahmad, A., & Maynard, S. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. *PACIS 2010* Proceedings, 43.

Lin, H.-F. (2008). Empirically testing innovation characteristics and organizational learning capabilities in e-business implementation success Hsiu-Fen. *Internet Research*, *18*(1), 60–78. https://doi.org/10.1108/EL-01-2014-0022

Liu, P., & Yi, S. (2018). A study on supply chain investment decision-making and coordination in the Big Data environment. *Annals of Operations Research*, *270* (1–2), 235–253. https://doi.org/10.1007/s10479-017-2424-4

Liu, Y., & Greene, C. (2020). The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination. In *Digital Transformation in Business and Society* (pp. 145–153).

https://doi.org/10.1007/978-3-030-08277-2
Loebbecke, C., & Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *Journal of Strategic Information Systems*, *24*(3), 149–157. https://doi.org/10.1016/j.jsis.2015.08.002
Loukaka, A., & S. M. Rahman, S. (2017). Discovering New Cyber Protection Approaches from a Security Professional Prospective. *International Journal of Computer Networks & Communications*, *9*(4), 13–25. https://doi.org/10.5121/ijcnc.2017.9402
Lu, R., Zhu, H., Liu, X., Liu, J., & Shao, J. (2014). Toward efficient and privacy-preserving computing in big data era. *IEEE Network*, *28*(4), 46–50. https://doi.org/10.1109/MNET.2014.6863131
Malik, P. (2013). Governing Big Data: Principles and practices. *IBM Journal of Research and Development*, *57*(3), 1:1-1:13. https://doi.org/10.1147/JRD.2013.2241359
March, J. G. (1991). Exploration and Exploitation in Organizational Learning. *Organization Science*, *2*(1), 71–87.
Markus, M. L. (1983). Power , Politics , and MIS Implementation. *Communications of the ACM*, *26*(6), 430–444.
Markus, M. L. (2015). New games, new rules, new scoreboards: the potential consequences of big data. *Journal of Information Technology*, *30*(1), 58–59. https://doi.org/10.1057/jit.2014.28
Martin, K. E. (2015). Ethical Issues in the Big Data Industry. *MIS Quarterly Executive*, *14*(2), 67–85.
Mayer-Schönberger, V., & Cukier, K. N. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York, New York, USA: Houghton Mifflin Harcourt Publishing.
Mayo, R. M., Summey, J. F., Williams, J. E., Spence, R. A., Kim, S., & Jagsi, R. (2017). Qualitative Study of Oncologists' Views on the CancerLinQ Rapid Learning System. *Journal of Oncology Practice*, *13*(3), e176–e184. https://doi.org/10.1200/jop.2016.016816
Mazzei, M. J., & Noble, D. (2017). Big data dreams: A framework for corporate strategy. *Business Horizons*, *60*(3), 405–414. https://doi.org/10.1016/j.bushor.2017.01.010
Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A Conceptual Framework for Threat Assessment Based on Organization ' s Information Security Policy. *Journal of Information Security*, *5*(October), 166–177.
Mennecke, B., Tan, C., Crompton, M., Smith, H. J., Shroff, M., & George, J. F. (2014). Privacy in the Age of Big Data : The Challenges and Opportunities for Privacy Research. *Thirty Fifth International Conference on Information Systems*, 1–5.
Miele, S., Shockley, R. (2013). *Analytics : The real-world use of big data*. Retrieved from https://www.informationweek.com/pdf_whitepapers/approved/1372892704_analytics_the_real_world_use_of_big_data.pdf
Miles, M. B., & Huberman, A. M. (2014). *Qualitative Data Analysis: An Expanded Sourcebook* (3rd editio). California: Sage Publications.
Miller, H. G., & Mork, P. (2013). From Data to Decisions : A Value Chain for Big Data. *IT Professional*, *15*(1), 57–59.
Mishra, D., Gunasekaran, A., Papadopoulos, T., & Childe, S. J. (2018). Big Data and supply chain management: a review and bibliometric analysis. *Annals of Operations Research*, *270*(1–2), 313–336. https://doi.org/10.1007/s10479-016-2236-y
MIT Technology Review. (2015). Securing the Big Data Life Cycle. In *MIT Technology Review Custom*.
Mohamad, M., Selamat, A., & Salleh, K. A. (2019). An analysis on deep learning approach performance in classifying big data set. *Proceedings - 2019 1st International Conference*

on Artificial Intelligence and Data Sciences, AiDAS 2019. https://doi.org/10.1109/AiDAS47888.2019.8970980

Moura, J., & Serrao, C. (2016). Security and Privacy Issues of Big Data. In *Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence* (Vol. 2). https://doi.org/10.4018/978-1-4666-8505-5.ch002

Nambisan, S., & Wang, Y. (1999). Roadblocks to Web Technology. *Communications of the ACM*, *42*(1), 1997–2000.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. *ACM International Conference Proceeding Series*, *Part F1282*, 56–60. https://doi.org/10.1145/3077584.3077593

Nasser, T., & Tariq, R. S. (2015). Big Data Challenges. *Journal of Computer Engineering & Information Technology*, *4*(3), 31–40. https://doi.org/10.4172/2324-9307.1000133

Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. In *Industrial Management & Data Systems* (Vol. 112). https://doi.org/10.1108/02635571211210059

NewVantage Partners. (2019). *Big Data and AI Executive Survey 2020*. Retrieved from www.newvantage.com

Nguyen, T., & Petersen, T. E. (2017). Technology Adoption in Norway: Organizational Assimilation of Big Data. Retrieved from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2455449/masterthesis.PDF?sequence=1

Oliveira, T., & Martins, M. F. (2011). Literature Review of Information Technology Adoption Models at Firm Level. *The Electronic Journal Information Systems Evaluation*, *14*(1), 110–121.

Olszak, C. M., & Mach-Król, M. (2018). A conceptual framework for assessing an organization's readiness to adopt big data. *Sustainability (Switzerland)*, *10*(10). https://doi.org/10.3390/su10103734

Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007). Employees ' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, 1–10.

Park, J. H., & Kim, Y. B. (2019). Factors Activating Big Data Adoption by Korean Firms. *Journal of Computer Information Systems*, *0*(0), 1–9. https://doi.org/10.1080/08874417.2019.1631133

Patil, R. (2014). Supermarket Tesco pioneers Big Data - Dataconomy. Retrieved from Dataconomy website: http://dataconomy.com/tesco-pioneers-big-data/

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big Data Privacy in the Internet of Things Era. *IT Professional*, *17*(3), 32–39. https://doi.org/10.1109/MITP.2015.34

Perreault, L. (2015). Big Data and Privacy. *Conf-IRM 2015 Proceedings*. 15. Retrieved from https://aisel.aisnet.org/confirm2015/15

Chen, C. L., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, *275*, 314–347. https://doi.org/10.1016/j.ins.2014.01.015

Phillips-Wren, G., Iyer, L. S., Kulkarni, U., & Ariyachandra, T. (2015). Business analytics in the context of big data: A roadmap for research. *Communications of the Association for Information Systems*, *37*, 448–472.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-

9010.88.5.879
Prakash, A. A., Prithiviraj, S., & Mary, R. (2018). Review on Big Data Security Management. *International Journal for Research in Applied Science & Engineering Technology*, *6*(3), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004
Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management*, *38*(1), 187–195. https://doi.org/10.1016/j.ijinfomgt.2017.07.008
Ranum, M. (2014). Free-Form Versus Off-the-Shelf: Big Data Security Still a Ways Off. *Information Security*, (April), 9–13.
Rehman, S. U. R., & Qingren, C. A. O. (2017). A qualitative study of the challenges faced by organizations in Big Data Implementation. *International Journal of Modern Research in Management*, *1*(1), 1–13.
Richardson, R. (2013). Big Data Creates Cloudy Security Forecast. *Information Security*, (March), 2–4.
Robey, D., Ross, J. W., & Boudreau, M. . (2000). Learning to Implement Enterprise Systems : An Exploratory Study of the Dialectics of Change Learning to Implement Enterprise Systems : An Exploratory Study of the Dialectics of Change. *Journal of Management Information Systems*, *1*(19), 1–48. https://doi.org/10.1080/07421222.2002.11045713
Rogers, E. M. (2003). Diffusion of Innovations. In *New York Free Press* (Vol. 21). Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/12369480
Rosli, K. (2012). Computer-Assisted Auditing Tools Acceptance Using I-Toe : A New Paradigm. *PACIS 2012*, Paper 195.
Rubinstein, I. S. (2012). *Big Data : The End of Privacy or a New Beginning ?* Retrieved from http://lsr.nellco.org/nyu_plltwp/357
Rubinstein, S. M, Warner, J. L. (2018). CancerLinQ : Origins , Implementation , and Future Directions. J*CO Clinical Cancer Informatics*, 2, 1-7
Saenz, C. F. L., Chang, Y., Kim, J., & Park, M. (2013). Exploring Big Data Challenges : Factors Affecting Individuals ' Intention For Authorizing Their Network Operators The Usage Of Their Personal Information. *PACIS 2013* Proceedings, 110.
Salahshour Rad, M., Nilashi, M., & Mohamed Dahlan, H. (2018). Information technology adoption: a review of the literature and classification. *Universal Access in the Information Society*, *17*(2), 361–390. https://doi.org/10.1007/s10209-017-0534-z
Salleh, K. A., & Janczewski, L. (2016). Technological, Organizational and Environmental Security and Privacy Issues of Big Data: A Literature Review. *Procedia Computer Science*, *100*. https://doi.org/10.1016/j.procs.2016.09.119
Samet, R., Aydin, A., & Toy, F. (2019). Big Data Security Problem Based on Hadoop Framework. *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, 525–530. https://doi.org/10.1109/UBMK.2019.8907074
Samuel, A., Sarfraz, M. I., Haseeb, H., Basalamah, S., & Ghafoor, A. (2015). A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data. *IEEE Transactions on Multimedia*, *17*(9), 1484–1494. https://doi.org/10.1109/TMM.2015.2458299
Sans Institute. (2015). *Enabling Big Data by Removing Security and Compliance Barriers*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/membership/36017
Sapio Research. (2019). *Big Data Survey - Unravel*. Retrieved from https://info.unraveldata.com/lp-research-big-data-survey-2019.html
Saraladevi, B., Pazhaniraja, N., Paul, P. V., Basha, M. S. S., & Dhavachelvan, P. (2015). Big data and Hadoop-A study in security perspective. *Procedia Computer Science*, *50*, 596–601. https://doi.org/10.1016/j.procs.2015.04.091

Schlienger, T. (2003). Analyzing Information Security Culture : Increased Trust by an Appropriate Information Security Culture. *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*.

Shahbaz, M., Zhai, L., Shahzad, F., Hu, Y., & Gao, C. (2019). Investigating the adoption of big data analytics in healthcare: the moderating role of resistance to change. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0170-y

Shannon-Baker, P. (2016). Making Paradigms Meaningful in Mixed Methods Research. *Journal of Mixed Methods Research*, *10*(4), 319–334. https://doi.org/10.1177/1558689815575861

Sharif, A., Cooney, S., Gong, S., & Vitek, D. (2015). Current security threats and prevention measures relating to cloud services, Hadoop concurrent processing, and big data. *Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data 2015*, 1865–1870. https://doi.org/10.1109/BigData.2015.7363960

Shatnawi, M. Q., Yassein, M. B., Abuein, Q., & Nsuir, L. (2019). Big data analytics tools and applications: Survey. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3368691.3368741

Sheng, J., Amankwah-Amoah, J., & Wang, X. (2017). A multidisciplinary perspective of big data in management research. *International Journal of Production Economics*, *191*(June), 97–112. https://doi.org/10.1016/j.ijpe.2017.06.006

Shim, J. P., French, A. M., & Jablonski, J. (2015). Big Data and Analytics: Issues, Solutions, and ROI. *Communications of the Association for Information Systems*, *37*(10), 797–810.

Simms, D. (2015). Big Data, Unstructured Data, and the Cloud: Perspectives on Internal Controls. In F. Xhafa, L. Barolli, A. Barolli, & P. Papajorgji (Eds.), *Modeling and Processing for Next-Generation Big-Data Technologies* (pp. 319–340). https://doi.org/10.1007/978-3-319-09177-8

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644–667.

Singh, M., Halgamuge, M. N., Ekici, G., & Jayasekara, C. S. (2018). A Review on Security and Privacy Challenges of Big Data. In *Cognitive Computing for Big Data Systems Over IoT, Lecture Notes on Data Engineering and Communications Technologies 14* (pp. 175–200). https://doi.org/10.1007/978-3-319-70688-7_8

Sivarajah, U., Irani, Z., Gupta, S., & Mahroof, K. (2020). Role of big data and social media analytics for business to business sustainability: A participatory web context. *Industrial Marketing Management*, *86*, 163–179. https://doi.org/10.1016/j.indmarman.2019.04.005

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research*, *70*, 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001

Soliman, O. H. (2019). Big Data SAVE: Secure Anonymous Vault Environment. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, *6*, 7098–7107. https://doi.org/10.24251/hicss.2019.852

Srivastava, U., & Gopalkrishnan, S. (2015). Impact of big data analytics on banking sector: Learning for Indian Banks. *Procedia Computer Science*, *50*, 643–652. https://doi.org/10.1016/j.procs.2015.04.098

Su, C. (2019). Big data security and privacy protection. *Proceedings - 2019 International Conference on Virtual Reality and Intelligent Systems, ICVRIS 2019*, 87–89. https://doi.org/10.1109/ICVRIS.2019.00030

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2016). Understanding the Factors Affecting the Organizational Adoption of Big Data. *Journal of Computer Information Systems*, *00*(00), 1–11. https://doi.org/10.1080/08874417.2016.1222891

Swanson, E. B. (1994). Information systems innovation among organizations. *Management Science*, *40*(9), 1069–1088.

Tafti, M. H. A. (2005). Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, *105*(5), 549–560.

Tankard, C. (2012). Big data security. *Network Security*, *2012*(7), 5–8. https://doi.org/10.1016/S1353-4858(12)70063-6

Teddlie, C., & Tashakkori, A. (2009). Foundations of Mixed Methods Research: Integrating Qualitative and Quantitative Approaches in the Social and Behavioral Sciences. London: Sage Publications.

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: an institutional perspective. *MIS Quarterly*, *27*(1), 19–49.

Teo, T. S. H., Ranganathan, C., & Dhaliwal, J. (2006). Key Dimensions of Inhibitors for the Deployment Commerce. *IEEE Transactions on Engineering Management*, *53*(3), 395–411.

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2016). A survey on security and privacy issues in big data. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, (September 2018), 202–207. https://doi.org/10.1109/ICITST.2015.7412089

Thales, 451 Research. (2018). *2018 Thales Data Threat Report: Trends in Encryption and Data Security, US Finance Edition*. Retrieved from https://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Thales-Data-Threat-Report-Financial-Services-es.pdf

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, *EM-29*(1), 28–45. https://doi.org/10.1109/TEM.1982.6447463

Torre, M. La, Dumay, J., & Rea, M. A. (2018). Breaching intellectual capital: critical reflections on Big Data security. *Meditari Accountancy Research*, *26*(3), 463–482. https://doi.org/http://dx.doi.org/10.1108/MRR-09-2015-0216

Trustwave. (2013). *2013 Global Security Report*. Retrieved from http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Van der Aalst, W., & Damiani, E. (2015). Processes Meet Big Data: Connecting Data. *IEEE Transactions on Services Computing*, *1*(1), 1–1. https://doi.org/10.1109/TSC.2015.2493732

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Research in Information Systems. *Management Information Systems Quaterly*, *37*(1), 21–54.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2014). *User Acceptance of Information Technology : Toward a Unified View*. *27*(3), 425–478.

Venkatesh, V., Morris, M. G., Hall, M., Davis, G. B., Davis, F. D., & Walton, S. M. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Venkatraman, S., & Venkatraman, R. (2019). Big data security challenges and strategies. *AIMS Mathematics*, *4*(3), 860–879. https://doi.org/10.3934/math.2019.3.860

Verma, S., Bhattacharyya, S. S., & Kumar, S. (2018). An extension of the technology acceptance model in the big data analytics system implementation environment. *Information Processing and Management*, *54*(5), 791–806. https://doi.org/10.1016/j.ipm.2018.01.004

Walker, R. S., & Brown, I. (2019). Big data analytics adoption : A case study in a large South

African telecommunications organisation. *South African Journal of Information Management*, *21*(1), 1–10.

Wang, H., Jiang, X., & Kambourakis, G. (2015). Special issue on Security, Privacy and Trust in network-based Big Data. *Information Sciences*, *318*, 48–50. https://doi.org/10.1016/j.ins.2015.05.040

Wang, Y.-M., Wang, Y.-S., & Yang, Y.-F. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. *Technological Forecasting and Social Change*, *77*(5), 803–815. https://doi.org/10.1016/j.techfore.2010.03.006

Watson, H. J. (2014). Tutorial: Big Data Analytics: Concepts, Technologies, and Applications. *Communications of the Association for Information Systems*, *34*, 24.

Watson, H. J. (2019). Update tutorial: Big data analytics: Concepts, technology, and applications. *Communications of the Association for Information Systems*, *44*(1). https://doi.org/10.17705/1CAIS.04421

Wielki, J. (2015). The Opportunities and Challenges Connected with Implementation of the Big Data Concept. In M. Mach-Król, C. M. Olszak, & T. Pełech-Pilichowski (Eds.), *Advances in ICT for Business, Industry and Public Sector* (pp. 171–189). https://doi.org/10.1007/978-3-319-11328-9

Wood, P. (2013, March). How to tackle big data from a security point of view. *Computer Weekly*. Retrieved from http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yadegaridehkordi, E., Hourmand, M., Nilashi, M., Shuib, L., Ahani, A., & Ibrahim, O. (2018). Influence of big data adoption on manufacturing companies' performance: An integrated DEMATEL-ANFIS approach. *Technological Forecasting and Social Change*, *137*(March), 199–210. https://doi.org/10.1016/j.techfore.2018.07.043

Yang, L., Li, J., Elisa, N., Prickett, T., & Chao, F. (2019). Towards Big data Governance in Cybersecurity. *Data-Enabled Discovery and Applications*, *3*(1), 1–12. https://doi.org/10.1007/s41688-019-0034-9

Yin, H., Jiang, Y., Lin, C., Luo, Y., & Liu, Y. (2014). Big Data: Transforming the Design Philosophy of Future Internet. *IEEE Network*, *28*(4), 14–19.

Yin, R. K. (2009). Case Study Research: Design and Methods. In *Essential guide to qualitative methods in organizational research* (Vol. 5). https://doi.org/10.1097/FCH.0b013e31822dda9e

Young, R. (2010). Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security. *Journal of International Technology and Information Management*, *19*(3), 19–37. Retrieved from http://search.proquest.com.ezproxy.auckland.ac.nz/docview/859111188/fulltextPDF?accountid=8424

Zaki, T., Uddin, M. S., Hasan, M. M., & Islam, M. N. (2017). Security threats for big data: A study on Enron e-mail dataset. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6. https://doi.org/10.1109/ICRIIS.2017.8002481