Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2015 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2015

SEC-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption

Khairulliza Ahmad Salleh
University of Auckland, k.salleh@auckland.ac.nz

Lech Janczewski
University of Auckland, lech@auckland.ac.nz

Fernando Beltran
University of Auckland, f.beltran@auckland.ac.nz

SEC-TOE FRAMEWORK: EXPLORING SECURITY DETERMINANTS IN BIG DATA SOLUTIONS ADOPTION

Khairulliza Ahmad Salleh, Department of Information Systems and Operations Management, University of Auckland, Auckland, New Zealand, k.salleh@auckland.ac.nz

Lech Janczewski, Department of Information Systems and Operations Management, University of Auckland, Auckland, New Zealand, l.janczewski@auckland.ac.nz

Fernando Beltran, Department of Information Systems and Operations Management, University of Auckland, Auckland, New Zealand, f.beltran@auckland.ac.nz

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

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 (Mayer-Schönberger & Cukier 2013; Demchenko et al. 2014). 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. Else, 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 et al. 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 2, followed by the proposed hypotheses and conceptual research framework in section 3. Section 4 presents the proposed research design and section 5 concludes the paper with expected contributions of the research.

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.

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) for 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.

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 outlet 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.

2.3 Theoretical Foundation

2.3.1 Technological-Organizational-Environmental (TOE) Framework

TOE framework was first introduced by Tornatzky and Fleischer in a book titled *The Processes of Technological Innovation* (Tornatzky & Fleischer 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. Essentially, it is believed that the fit between the existing technology setting in a firm and the intended technology innovation will be the 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" (Tornatzky & Fleischer 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).

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 is 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? (pre-post measures)
4. What recommendation on security management aspects could 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.

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.

3.1 Technology Factors in Security

3.1.1 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.

3.1.2 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 (Kwon & Zmud 1987; Borgman et al. 2013). 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.

3.2 Organizational Factors in Security

3.2.1 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 et al. 2012; Knapp et al. 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 et al. 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.

3.2.2 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 et al. 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.

3.2.3 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 means 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.

3.3 Environmental Factors in Security

3.3.1 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 et al. 2014). Thus, it is posited that:

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

3.3.2 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 et al. 2012; Trustwave 2013). Thus, this research posits that:

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

3.4 Interrelation between constructs

3.4.1 Organizational Learning Culture and Perceived Complexity

From innovation perspective, organizations tend to use present knowledge as a foundation to apply the knowledge into new activities or processes. Hence, organizational ability to adopt knowledge intensive technology is closely linked to the availability of organizational knowledge and learning process on the technology (Nambisan & Wang 1999). For organizations that have positive learning orientation, organizational view towards the perceived complexity of certain technology innovation will be more optimistic. This is due to organizational ability to sense and respond to knowledge deficits on the intended technology adoption. It is believed that learning orientation influences the ability of an organization to support complex innovations, and reflects that the organization values knowledge, is open minded, and has a shared vision (Baker & Sinkula 1999). This leads to the following hypothesis:

H8: Organizational learning culture will positively affect perceived complexity of big data solutions.

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

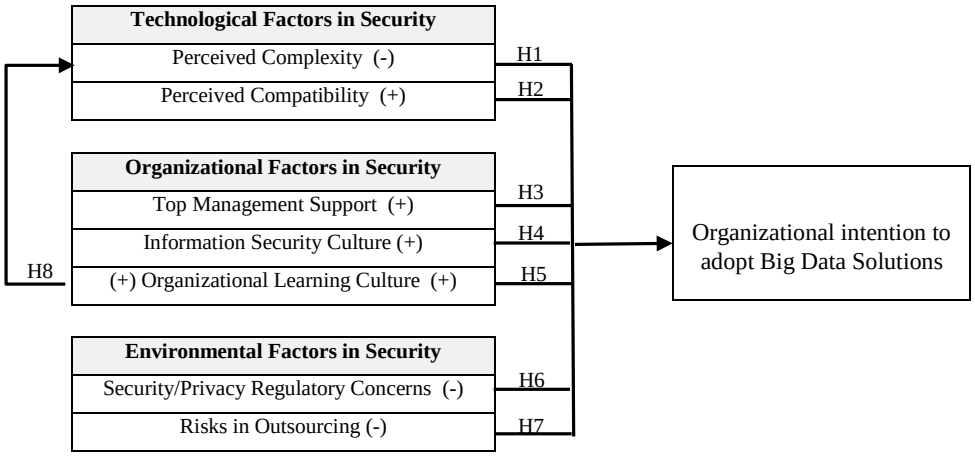

Figure 1. Sec-TOE Framework – Security determinants in BDS adoption

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 2007). 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 as representers for 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 2007).

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.

References

Baker, W.E. & Sinkula, J.M., (1999). Learning orientation, market orientation, and innovation: Integrating and extending models of organizational performance. *Journal of Market-Focused Management*, 4(4), pp.295–308.

Bansal, A., Kaur, A. & Aggarwal, A., (2014). BIG DATA EXPLOSION: INSIGHT FOR NEW AGE MANAGERS. , 5(5), pp.7–11.

Big Data Working Group, (2013). *Expanded Top Ten Big Data Security and Privacy Challenges*, Available at: https://cloudsecurityalliance.org/download/expanded-top-ten-big-data-security-and-privacy-challenges/

Borgman, H.P. et al., (2013). Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. In *2013 46th Hawaii International Conference on System Sciences*. Ieee, pp. 4425–4435.

Creswell, J.W. & Clark, V.L.P., (2007). *Designing and conducting mixed methods research*, Thousand Oaks, Calif, SAGE Publications.

Cumbley, R. & Church, P., (2013). Is "Big Data" creepy? *Computer Law & Security Review*, 29(5), pp.601–609.

Davenport, T.H., (2014). *Big Data at Work: Dispelling the Myths, Uncovering the Opportunities*, Massachusetts: Harvard Business School Publishing Corporation.

Demchenko, Y. et al., (2014). Big Security for Big Data: Addressing Security Challenges for the Big Data Infrastructure. In W. Jonker & M. Petković, eds. *Secure Data Management*. Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 76–94.

Dhillon, G., (1997). *Managing Information System Security*, Houndmills, Basingstoke, Hampshire: MacMillan Press Ltd.

Fichman, R.G. & Kemerer, C.F., (1997). The Assimilation Of Software Process Innovations: An Organizational Learning Perspective. *Management Science*, 43(10), pp.1345–1363.

Gartner Inc, 2012. *The Importance of ' Big Data ': A Definition*, Available at: https://www.gartner.com/doc/2057415/importance-big-data-solution

Göb, R.,(2014). Discussion of "Reliability Meets Big Data: Opportunities and Challenges." *Quality Engineering*, 26(1), pp.121–126. Available at: http://www.tandfonline.com/doi/abs/10.1080/08982112.2014.846124 [Accessed August 21, 2014].

Hashem, I.A.T. et al., (2014). The rise of "Big Data" on cloud computing: Review and open research issues. *Information Systems*, 47, pp.98–115.

Hayashi, K., (2013). Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility. In *2013 International Conference on Availability, Reliability and Security*. Ieee, pp. 506–511.

Hu, Q. et al., (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences*, 43(4), pp.615–660.

IDC, (2015). *Asia / Pacific Big Data Technology and Services 2014 – 2018 Analysis and Forecast*, Available at: http://www.idc.com/getdoc.jsp?containerId=AP250914

IDC, (2013). New IDC Worldwide Big Data Technology and Services Forecast Shows Market Expected to Grow to $32 billion in 2007. Available at: http://www.idc.com/getdoc.jsp?containerId=prUS24542113.

IDG Enterprise, (2014). *Big Data: A Survey*, Available at: http://www.idgenterprise.com/report/big-data-2

Jagadish, H. V. et al., (2014). Big data and its technical challenges. *Communications of the ACM*, 57(7), pp.86–94. Available at: http://dl.acm.org/citation.cfm?doid=2622628.2611567.

Kankanhalli, A. et al., (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), pp.139–154. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401202001056 [Accessed December 27, 2014].

Kim, G.-H., Trimi, S. & Chung, J.-H., (2014). Big-data applications in the government sector. *Communications of the ACM*, 57(3), pp.78–85.

Knapp, K.J. et al., (2004). *Top Ranked Information Security Issues : Certification Consortium (ISC) 2 Survey Results*, Auburn, Alabama.

Kshetri, N., (2014). Big data′s impact on privacy, security and consumer welfare. *Telecommunications Policy*, pp.1–12.
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), pp.387–394.
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.
March, J.G., (1991). Exploration and Exploitation in Organizational Learning. *Organization Science*, 2(1), pp.71–87.
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.
Nambisan, S. & Wang, Y., (1999). Roadblocks to Web Technology. *Communications of the ACM*, 42(1), pp.1997–2000.
Nassimbeni, G., Sartor, M. & Dus, D., (2012). *Security risks in service offshoring and outsourcing*, Available at: http://www.emeraldinsight.com/doi/abs/10.1108/02635571211210059 [Accessed December 23, 2014].
Van Niekerk, J.F. & Von Solms, R., (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), pp.476–486.
Pahnila, S. et al., (2007). Employees ' Behavior towards IS Security Policy Compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. pp. 1–10.
Rubinstein, I.S., (2012). *Big Data : The End of Privacy or a New Beginning ?*, International Data Privacy Law (2013 Forthcoming); NYU School of Law, Public Law Research Paper No. 12-56.
Schlienger, T., (2003). Analyzing Information Security Culture : Increased Trust by an Appropriate Information Security Culture. In *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*.
Singh, A.N., Gupta, M.P. & Ojha, A., (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, 27(5), pp.644–667.
Tankard, C., (2012). Big data security. *Network Security*, 2012(7), pp.5–8. Available at: http://dx.doi.org/10.1016/S1353-4858(12)70063-6.
Teo, T.S.H., Ranganathan, C. & Dhaliwal, J., (2006). Key Dimensions of Inhibitors for the Deployment Commerce. *IEEE transactions on Engineering Management*, 53(3), pp.395–411.
Tornatzky, L.G. & Fleischer, M., (1990). *The processes of technological innovation*, Lexington Books.
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), pp.28–45.
Trustwave, (2013). *2013 GLOBAL SECURITY REPORT*, Available at: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.
Da Veiga, a. & Eloff, J.H.P., (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp.196–207.
Wood, P., (2013). How to tackle big data from a security point of view. *Computer Weekly*. Available at: 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), pp.2799–2816.