8-2019

Three Essays on Information Security Breaches and Big Data Analytics: Accounting and Auditing Perspective

Shariful Islam

THREE ESSAYS ON INFORMATION SECURITY BREACHES AND BIG DATA ANALYTICS: ACCOUNTING AND AUDITING PERSPECTIVE

by

Md. Shariful Islam, B.B.A., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

August 2019

LOUISIANA TECH UNIVERSITY

GRADUATE SCHOOL

May 29, 2019
Date of dissertation defense

We hereby recommend that the dissertation prepared by

Md. Shariful Islam

entitled **Three Essays on Information Security Breaches and Big Data Analytics: Accounting and Auditing Perspective**

be accepted in partial fulfillment of the requirements for the degree of

Doctor of Business Administration, Computer Information Systems Concentration

Dr. Thomas Stafford, Supervisor of Dissertation Research

Dr. Selwyn Ellis,
Head of Computer Information Systems

Members of the Doctoral Committee:
Dr. William Stammerjohan
Dr. Selwyn Ellis

Approved:

Christopher Martin
Dean of Business

Approved:

Ramu Ramachandran
Dean of the Graduate School

GS Form 13a
(01/19)

ABSTRACT

The dissertation examines two separate yet significant Information Technology (IT) issues: one dealing with IT risk and the other involving the adoption of IT. The IT risks that the dissertation focuses are information security breaches and the adoption/outsourcing of big data analytics. Using competitive dynamics theory and the theory of information transfer, the dissertation examines whether there is a spillover effect from information security breaches of breached firms to those firms' rivals. Market reaction from spillover effects is captured from market activity and information asymmetry. The results suggest that the market of rival firms react to the focal firm's experience of a data breach. However, the overall effects of data breaches on rival firms are the opposite to those to focal firms, although in many cases rival firms also experience negative reactions in the financial markets. Specifically, the results suggest that the characteristics of data breach types and previous data breach histories of focal firms have implications for rivals. However, strong information technology governance capabilities of rivals play a shielding role in mitigating those negative effects.

The dissertation also examines the adoption of big data analytics by Internal Audit Function (IAF). Particularly, the dissertation examines the implications of data analytics challenges to the adoption of big data analytics by IAF. The results suggest that data-specific IT knowledge rather than general IT knowledge is a significant predictor of adoption of big data analytics. Additionally, critical thinking skills and business

knowledge also contributes to the adoption of big data analytics. Furthermore, if IAFs face management challenges, such as fraud risk detection, they are also more likely to adopt big data analytics. Results from interaction effects analysis suggest that Chief Audit Executives (CAEs) with CPA certifications are more likely to adopt big data analytics than the CAEs without CPA certification, when the size of the organization is small, when the size of the IAF is small, or when there is a lack of data-specific IT knowledge or business skills. Another important finding is that when two groups of IAFs have similar size and data-specific IT knowledge, IAFs with fraud detection responsibilities are more likely to adopt big data analytics. Finally, IAFs in Anglo culture countries are more likely to adopt big data analytics than IAFs in non-Anglo culture countries, even when both IAFs have the same size and data-specific IT knowledge.

Finally, the dissertation examines the motivation of outsourcing of data analytics by IAF. The results suggest, contrary to conventional wisdom, that economic factors are not a significant predictor. Rather, strategic and sociological factors are significant in predicting the outsourcing of big data analytics. Specifically, IAFs outsource big data analytics when they lack data skills and are tasked with fraud risk management. Additionally, the role Chief Audit Executives (CAEs) is also significant. There is also a cultural variation of the outsourcing decision: IAFs from developing nations are more likely to outsource than are the IAFs from the developed countries. Further analysis of the interaction effects of these significant variables suggests that as the data skills of IAFs increase, the conditional difference of the likelihood of outsourcing decreases, suggesting that IAFs recognize both the value of data analytics and their lack of competencies. The three-way interactions of the variables support the same conclusion. The findings have

implications about the formation of effective internal controls designed to mitigate the risks in the outsourcing decision. Moreover, external auditors will find the results useful when they evaluate the competence and objectivity of IAFs before they rely on their work.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author_____

Date _____

GS Form 14
(5/03)

DEDICATION

To

My Parents,

Md. Shafi Uddin and Kohinoor Begum,

For their sacrifice, love, support, and strength.

To

My Wife

Nusrat Farah,

For her patience and understanding.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

I thank all of the people who encouraged me and laid the foundation for doctoral study.

I especially thank my dissertation chair and co-chair Dr. Tom Stafford and Dr. William Stammerjohan respectively for their guidance and wisdom during the dissertation phase of the doctoral study at Louisiana Tech University. Their support, enthusiasm, and scholarship have motivated me throughout the dissertation preparation process and will continue over the course of my career.

Dr. Selwyn Ellis deserves special thanks as the member of the dissertation committee. I thank Dr. William McCumber, Dr. Jun Duanmu, and Dr. Jared Egginton each for their help and guidance in the data analysis process of the dissertation.

I also owe gratitude to many faculty members of Louisiana Tech University who supported and encouraged me in different ways during my doctoral study.

CHAPTER 1

INTRODUCTION

Organizations are increasingly utilizing Information Technology (IT) resources for competitive advantages. Effective utilization of IT resources affects the bottom line of organizations. However, utilization of IT is not without risk; the landscape of IT risks is evolving. In this dissertation, I will focus on two significant IT issues: one is IT risk and the other is the challenge of adoption/outsourcing of an emerging IT. One risk which the dissertation focuses upon is the possibility of information security breaches; the other risk studied here is related to big data analytics particularly, the challenges inherent in adoption and outsourcing of big data analytics by auditors.

Information Security Breaches

Cyberattacks have become a common IT risk. However, until recently, such attacks and breaches were hardly discussed. For organizations, the implications for cyberattacks are no longer confined to server rooms; they have now become a very significant issue for board rooms. The Ponemon Institute (2017) reports that, on average, cyber-crime costs $11.7 million per company and that the number of security breaches firms experienced increased annually by 27.4%. Juniper Research (2015) estimates that by 2019 cybercrime will cost companies more than $2 trillion; a figure that is four times

the expenses estimated in 2015. Consumer market technology users are also concerned about data breaches. The Securities and Exchange Commission (2011) notes that "Registrants should address cybersecurity risks and cyber incidents in their Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Risk Factors, Description of Business, Legal Proceedings and Financial Statement Disclosures." These backdrops underlie the significance of research related to information security breaches.

Big Data Analytics

Big data analytics has recently become a buzzword in the literature. The Economist (2017) reports that the world's most valuable resource is no longer oil, but data. Today's vast amount of data provides companies with great opportunities to create competitive advantage, and research suggests that data-driven decision-making leads to significant differences in Return on Assets (ROA), Return on Equity (ROE), and firm productivity (Provost and Fawcett 2013). Investments in big data analytics signal greater potential for organizations. International Data Corporation (2015) forecasts that by 2019, organizations around the world will spend about $48.6 billion on big data analytics and related services.

Big data analytics is important for the accounting profession because data gathering and analysis technologies have the potential to fundamentally change accounting and auditing task processes (Schneider et al. 2015). It is noted that the emergence of big data analytics will significantly change the "infer (insight), predict (foresight), and assure (oversight) tasks" performed by accountants and auditors. Although statistics suggests that organizations (which is to say, the clients of accountants) have already moved to adopt big data analytics, accountants themselves are

lagging behind their clients in adopting the technology. Therefore, research related to the use of big data analytics by accountants/auditors is very important.

Research Questions and Motivations for the Research

Information Transfer of Information Security Breach

Cybersecurity research has focused on many aspects of IT uses, including behavioral issues of organizational insiders, security culture, and the economic significance of breaches in capital markets. Most studies dealing with the economic significance of data breaches focus on the market reactions of the investors in breached firms. For example, Campbell et al. (2003) examined the economic effect of information security breaches reported in press on the publicly listed companies in the US. Overall, they find limited evidence of negative market reactions to the announcement of information security breaches. However, cross-sectional analysis suggests that breach types, particularly the compromise of confidential information, can cause significant market reactions. Similarly, Acquisti, Friedman, and Telang (2006) documented significant market reaction following the announcement of security breaches. Overall, these studies suggest that data breaches have capital market consequences for the breached firms.

One noteworthy point of the studies that lead to this conclusion is that they studied only breached firms. However, theories suggest that market reactions to the announcement of data breaches are not confined to breached firms, alone, and can impact rival firms in the same marketplaces. Hence, there are potentially far-reaching effects. The theory of competitive dynamics suggests that firms related to breached firms are also

likely to be affected by the other firms' data breaches. There are two mechanisms through which this information transfer might spread – the contagion effect (rivals experience same effect of the breached firms) or competitive effect (rivals experience the opposite effect of the breached firms). The literature suggests that these kinds of information transfer occur for many other events as well, such as bankruptcy (Lang and Stulz 1992), accounting restatements (Gleason, Jenkins, and Johnson 2008), financial misconduct (Paruchuri and Misangyi 2015), or even environmental problems (Barnett and King 2008). Nevertheless, research related to the information transfer of security breach is sparse. Therefore, the first study of the dissertation seeks the answer to the question, "Is there any information transfer from security breaches from breached firm to related firms?"

Adoption of Big Data Analytics by Accountants/Auditors

Though big data analytics has significant implications for auditors and accountants, Earley (2015) suggests that significant hurdles need to be overcome in order to realize the benefits of data analytics. Existing literature has identified a number of challenges to the adoption of big data analytics (Sivarajah et al. 2017; Schneider et al. 2015). Some of these challenges include data challenges (skills), process challenges (cognition), and management challenges (organization). Skill challenges (i.e., data) imply that since data analytics is an emerging technology, existing IT skills might not suffice for the use of data analytics. Process challenges (i.e., cognition) challenges imply that big data poses challenges to the information process and thus requires high tolerance for ambiguity. Additionally, it is considered that extracting meaningful knowledge from big data requires not only a deep understanding of the data, but also a creative way of

thinking about the data. Finally, management challenges (i.e., organizational issues) implies that organizations will not mobilize themselves to adopt data analytics unless there are circumstances in which big data analytics can contribute significantly to operation. The second study of the dissertation seeks the answers to the question, "Do the challenges to the adoption of big data analytics have implications for auditors?"

Outsourcing of Big Data Analytics by Accountants/Auditors

Though data analytics has implications for accountants/auditors, a number of challenges to the adoption of data analytics might prevent accountants/auditors from using data analytics. In such circumstances, outsourcing might be a better option than internal adoption. Moreover, the scarcity of skilled personnel for data analytics and the severe competition between organizations for these same personnel might also lead accountants/auditors to outsource big data analytics.

The study of outsourcing of big data analytics by auditors is important because the auditors who provide input data for decisions on outsourcing data analytics will also be directly affected by the outcome of those decisions and must subsequently rely on the work performed by the chosen service organization; thus, the motivations of accounting personnel who provide the financial inputs to outsourcing decisions are highly relevant and must be carefully considered before outsourcing decisions are undertaken (Christ, Mintchik, et al. 2015). Further, Blaskovich and Mintchik (2011, 13) suggest that although research on the drivers of outsourcing has been conducted for several decades, the dynamic nature of technology continues to raise many interesting questions and offer fruitful avenues for research. Moreover, Christ et al. (2015) noted that outsourcing of information systems such as big data analytics and the potential outsourcing of the IT

function are not identical business practices. Therefore, accounting scholars should exercise caution and evaluate the similarity of contextual factors when considering whether to extrapolate results in the literature concerning outsourcing of the IT function to research findings on big data analytics outsourcing. To sum up, given the above backdrops, the study of the outsourcing of data analytics by auditors warrants further investigation.

Organization of the Dissertation

The dissertation consists of three separate studies related to IT risks and adoption/outsourcing of an emerging IT. The first study, "Reaction of the Investors of Rival Firms to the Information Security Breach of Focal Firms: Evidence from Market Activity and Information Asymmetry," deals with whether the markets of rivals firms of data breached firms react when the firms announce their data breaches. The second study, "Big Data Analytics Challenges and Internal Audit Function (IAF)'s Reliance on Big Data Analytics," identifies challenges to the adoption of data analytics and their implications for accountants and auditors for such adoption decisions. The third study, "Outsourcing of Big Data Analytics by Internal Audit Function (IAF)," focuses on the factors that lead IAF to outsource big data analytics. The last section of the dissertation summarizes the findings of the research and their implications for practitioners and academics.

CHAPTER 2

REACTION OF THE INVESTORS OF RIVAL FIRMS TO THE INFORMATION SECURITY BREACH OF FOCAL FIRMS: EVIDENCE FROM MARKET ACTIVITY AND INFORMATION ASYMMETRY

Introduction

Data breaches have become commonplace; every day companies fall victim to new and sophisticated types of exploits. In 2014, the number of average successful cyber-attacks per week was 160; a figure that is three times 2010 levels (Walters 2015). Ponemon Institute (2017) reports that, on average, cyber-crime costs $11.7 million per year per company and that the number of security breaches increased by 27.4%, annually. Juniper Research (2015) estimates that in 2019 cybercrime will cost companies more than a combined $2 trillion per year; a figure that is four times 2015 levels.

Regulators are also concerned about data breaches. The Securities and Exchange Commission (2011) noted that "Registrants should address cybersecurity risks and cyber incidents in their Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Risk Factors, Description of Business, Legal Proceedings and Financial Statement Disclosures," and the American Institute of Certified Public Accountants (2017) introduced a cyber-security risk management framework to facilitate reporting on data breach-related issues. HBGary (2013) reported

that 70% of investors are interested in the cybersecurity policies of organizations and that about 80% of investors are not likely to invest in firms with a data breach history. These findings emphasize the importance of studying organizational data breaches.

Much data breach research tests the economic significance of breaches. Specifically, these studies examine the reactions of the market (i.e., investors) when news of data breaches is made public either by the breached companies or by the press. Campbell et al. (2003) examined the economic effect of information security breaches reported in the press on the listed companies in the US. Overall, they found limited evidence of negative market reactions to the announcement of information security breaches. However, the cross-sectional analysis suggested that breach types, particularly breaches involving the compromise of confidential information, produce a significant market reaction. Hovav and D'Arcy (2003) studied the impact of Denial-of-Service (DOS) attack announcements on the market for a period of four and a half years. As was the case with Campbell et al. (2003), they did not identify any general market reaction; however, Internet-specific companies experienced more negative market reactions than other sorts of companies.

Hovav and D'Arcy (2004) studied the impact of virus attack announcements on the market value of affected firms and found that there is no overall significant impact of virus attack announcements on the share price of the affected companies. On the other hand, many studies do document negative market reactions to the announcement of data breaches. For example, Kannan, Rees, and Sridhar (2007) studied the cross sectional characteristics of different factors related to data breaches; these factors include the nature of the breach, the type of firm, and the time period of the study. Overall, the study

did not find any significant market reactions in response to breaches; however, market reactions were significant for the breaches that followed September 11, 2001. Moreover, market reactions for dot-com era data breaches were significantly different from those of the post dot-com era. Acquisti, Friedman, and Telang (2006) documented significant market reaction following the announcement of security breaches, and they further indicate that retail firms suffer more from the effects of breach announcements than other sorts of firms. Similarly, many other studies have attempted to document the economic effects of security breaches, but they have provided mixed results.

Theories suggest that market reactions to the announcement of data breaches are not confined to the breached firms, alone. Rather, there are far-reaching effects. The theory of competitive dynamics suggests that rival firms are also likely to be affected by announcements of data breaches of focal firms[1]. This information transfer between firms occurs through two different yet significant mechanisms: the contagion effect (influence similar to that experienced by the rival firm) or competitive effect (an effect opposite that of the rival's). The extant behavioral information security literature is silent on that nature and causes of such information transfer effects. Though very few studies focus on unaffected firms, it is likely that results from the few studies that have been conducted suffer from either generalization of the results or the reliability issues related to the measures of market reactions. Hinz et al. (2015) focused on the consumer electronics industry, but their sample size was only six companies. The results of the study suggest that the share price of both directly affected companies and related companies decreased. Zafar, Ko, and Osei-Bryson (2012) also studied both breached firms and non-breached

[1] Here, focal firms are the ones that have experienced security breaches.

firms, but they tried to document the financial impact by using corporate financial ratios, which are very unreliable measures of market reactions.

The study by Kannan, Rees, and Sridhar (2007) examined market reactions of breached firms and matched control firms; therefore, their results are not directly applicable for understanding rival firm market reactions. Furthermore, Cavusoglu, Mishra, and Raghunathan (2004) studied market reaction of breached firms and their Internet security suppliers, the results of which are also not generalizable to rivals of the breached firms. Ettredge and Richardson (2003) studied information transfer in the late dot-com era in which they classified their firms on the basis of the reliance on the Internet, which is not generalizable today because of the growing extent of data breaches and their increasingly significant impacts. More recently, Kashmiri, Nicol, and Hsu (2017) studied the information transfer of the Target Corporation data breach to other U.S. retailers in the same industry and found that there was a contagion effect from the Target data breach; in short, numerous U.S. retailers in Target's market segment suffered negative abnormal returns. The extent of the contagion effect in the Target case was conditioned on moderating factors such as company size and product market similarity, governance-related strength, information-technology related ability, marketing ability, and corporate social responsibility. The limitation of the study is that it examined only a single data breach, and thus lacks appreciable external validity. Similarly, Martin, Borah, and Palmatier (2017) found that data breaches of focal firms have a negative spillover effect for rival firms, also suggesting a contagion effect. However, Jeong, Lee, and Lim (2018) have found that data breaches of focal firms have a competitive effect on their rivals. These findings are in contrast with those of Kashmiri, Nicol, and Hsu (2017) and

Martin, Borah, and Palmatier (2017). All of these researchers studied abnormal returns. However, this dissertation study examines abnormal turnover and the bid-ask spread to measure the market reaction of rival firms; these metrics capture changes in the expectations of individual investors, and they are more powerful than simple price tests. Taken together, this backdrop suggests that there is a research gap for the effect of data breaches on non-breached firms, particularly for rival firms using more reliable market metrics that will better capture the reactions of the markets.

Using data from privacyrights.org, COMPUSTAT, CRSP, and BOARDEX, I find evidence that markets of rival firms react when competing firms experience data breaches. While the overall effects of data breaches for focal firms are opposite those of rival firms, in many cases rival firms' markets also react negatively. Specifically, the characteristics of data breach type and previous data breach history of focal firms have implications for the impact on their rivals. However, strong information technology governance on the part of rivals plays a shielding role in mitigating those negative effects. Further, though it is hypothesized that strategic similarities of breached firms to their rivals also has implications, results do not document this effect. Even so, the results of the study are robust to alternative specification of both the models and the sample.

The study contributes to the literature in several ways. First, the study contributes to the literature on information transfer analysis between firms; the previous literature established that information does transfer between the investors of different firms. In the context of data breaches, however, very few studies focus on the influence of information transfer about data breaches between firms. The few extant studies suffer from limitations in external validity and measurement, thus limiting their generality. Since the sample

used in this study covers a wide range of industries and employs different market metrics, it fills the void left by prior research.

In a second major contribution, this study is the first to focus on stock trading volume and the bid-ask spread as a measure of the market reactions of rival firms to data breaches of focal firms. On the one hand, equities pricing signals the average belief of investors about a given company and its current status. On the other hand, equities trading volume represents the total of individual investors' trades (Bamber and Cheon 1995) and can, in that sense, serve as an indicator of overall market sentiment about the focal company. Therefore, trading volume might identify information content that is cancelled out in the average pricing process and vice versa (Bamber and Cheon 1995). For that reason, trading volume analysis complements rather than substitutes for pricing analysis. Additionally, the focus on trading volume may enable us to capture the differences between individual and institutional investors which are averaged out in the pricing process, and, thus, provide a better test of the effects of information about a breach on the market of firms and their competitors (Chen and Sami 2008).

Third, there is a stream of research on the effects of information asymmetry in the markets of rival firms following data breaches of focal firms. Very few studies have focused on the information asymmetry effect of such data breaches, and it is generally considered that news of a data breach announcement should be completely unexpected (Rosati et al. 2017). For that reason, an abnormal bid-ask spread might be expected due to the information shock; this information shock creates higher uncertainty, and this will result in increasing the risk of exposure in informed market trading for stocks of focal firms. Moreover, because of the effects of information transfer between focal firms and

rivals, this same information asymmetry might be present in the markets of rival firms, as well.

Lastly, this study identifies factors that might have implications for rivals such as characteristics of data breaches and the previous history of data breaches for focal firms. The study suggests that the strong information technology governance of rival firms might help to mitigate negative consequences of focal firm data breaches. These results provide guidance for practitioners on ways to strengthen cybersecurity risk management programs in their organizations, which is considered an important step even for firms which are not yet affected by the data breaches in their markets.

Theoretical Background and Hypotheses Development

The research is based on theories drawn from the disciplines of finance, management and accounting. The first theoretical foundation of the research is based on the Efficient Market Hypothesis (EMH) of Fama (1970). According to the EMH, share prices reflect all possible available information about a firm. A firm's value at time t, expressed by V_t, can be written as the discounted present value of expected future cash flows given that all information is available:

$$V_t = E\left[\sum_{i=t}^{T} \frac{x_i \mid \emptyset_t}{\prod_{j=t}^{i}\left(1+r_j^t\right)}\right] \qquad \text{Eq. (2.1)}$$

In equation (2.1), E is the expectation, T represents the terminal period, $x_i \mid \emptyset_t$ is the expected net cash inflows in period *i* given that information $\emptyset_t$ is available at time *t*, and r_j^t is the cost (that is, the interest rate) faced by the firm in period *j* at time *t*. However, the market is often characterized by information asymmetry and such asymmetries can arise from data breaches. In such cases, investors learn about the data

breaches ($\emptyset_t$) from different sources, but most often from news media. This information leads investors to reassess their expectation about future cash flows.

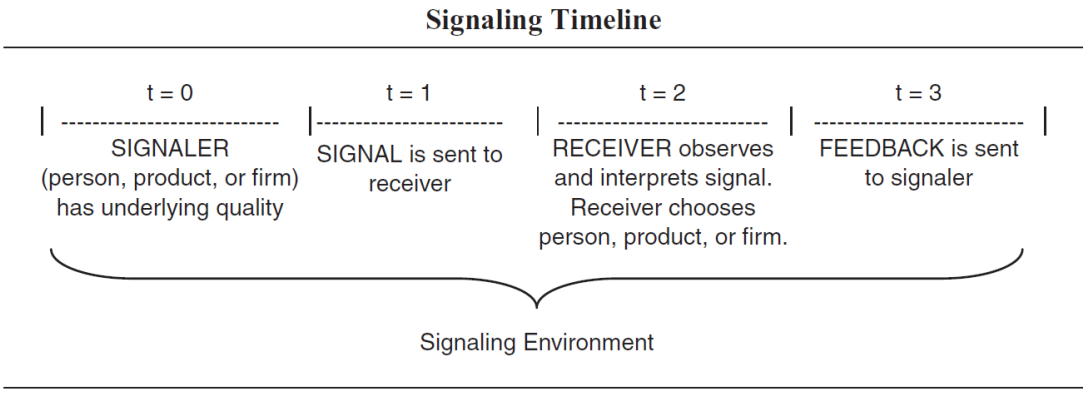
The second theoretical perspective on which the research draws is the theory of competitive dynamics. Under competitive dynamics, when information such as a firm's experience of a data breach is revealed to market, this revelation not only affects the breached companies but can also affect negatively the competitors in the industry, as well. This outcome is described as a contagion effect. Contagion effects are not limited to data breaches; they are known to occur in varying situations such as bankruptcy announcements (Lang and Stulz 1992), accounting restatements (Gleason, Jenkins, and Johnson 2008), news of financial misconduct (Paruchuri and Misangyi 2015), or an the occurrence of an environmental problem such as a chemical spill (Barnett and King 2008). In these instances, financial markets appear to adjust expectations downward for firms in the industry other than the focal firm (which is, of course, also impact), even when investment analysts do not alter their earnings forecasts. As in the case of communicable diseases, the contagion effect spreads from the affected firm to other firms in the industry, leading to industry-wide stock price declines (Arthurs et al. 2015).

Another school of thought related to competitive dynamics suggests that there is a theoretical possibility that competitor firms may actually *benefit* from a focal firm data breach. This school of thought is called the competitive effect. Prior literature related to different types of negative news about the organizations demonstrated support for this effect (Ferris, Jayaraman, and Makhija 1997; Haensly, Theis, and Swanson 2001). The competitive effect holds that when a focal firm is in distress, rivals in the industry configure their resources accordingly and that this competitive resource configuration is

perceived by investors in a positive light. The market's perception of the effect of negative news is revealed in the process of bidding for the rights to the residual cash flows among the firms in the industry. So, when one firm experiences a data breach, it is natural to assume that investors will bid up competitors' stocks, thus resulting in stock gains.

Actually, these competitive dynamics theories suggest that rival firms will always respond because they view the focal firm's data breach as a challenge and want to protect their own market positions, profitability, and financial market valuations. Additionally, they don't want to be considered a less valuable investment alternative to stakeholders (Farah 2017). However, the reactions of rivals are not uniform; their responses depend on many organizational and competitive factors. Some rivals might decide to respond aggressively to data breaches by taking a broad array of competitive actions. Others might decide not to respond, at all.

Signaling Theory holds that the announcement of an event about one party will provide other parties with information, thus permitting them to infer from the announcement. Signaling theory is widely used in economics, finance, and the accounting literature. In this school of thought, announcements of data breaches by focal firms serves to relay information to rivals. Rivals might perceive that they need take initiative to avoid such events in the future. Alternatively, they (the rivals) might also know that the susceptibility of focal firms might be perceived as a benefit by the rivals. In the literature related to finance, economics, and accounting, there are numerous studies that support signaling theory perspectives. Connelly et al. (2011) described the signaling theory effect in the following way:



Note: t = time.

Figure 2.1 *Signaling Theory Effect*

As discussed, rival firms are likely to respond to the focal firm's data breaches. However, defining the nature of what constitutes "rival firms" is critical. Here, I will define rivals using the Text-Based Network Industry Classification (TNIC) approach developed by Hoberg and Phillips (2010, 2016), who use topic modeling to identify rivals. Other studies have also used the same method to identify rivals for investigation (Sheikh 2018; Collins, Kim, and Ohn 2018).

I first measure the reaction of the market by using trading volume data. The literature suggests that the trading volume metric captures changes in the expectations of individual investors and that it is a more powerful test than price tests (Bamber, Barron, and Stevens 2011). Moreover, where stock price reactions are determined by the average investor's beliefs about a specific event, trading volume reaction arises from heterogeneous beliefs about the future price trends among individual investors (Beaver 1968); trading volume reactions can exist without price reactions, and vice versa (Bamber and Cheon 1995). However, trading volume better captures the differences between individual investors and institutional investors that may be cancelled out in price analysis (Chen and Sami 2013). Trading volume reaction is also more powerful than price

reactions in small sample settings, as well (Cready and Hurtt 2002; Cready and Mynatt 1991). Experimental studies of trading volume also suggest that trading activity around announcements should increase/decrease in reaction to the magnitude of the news characterized by such announcements (Gillette et al. 1999), a finding that is consistent with Kim and Verrecchia (1991).

Second, I measure the reaction of investors to the data breach of focal firms using a bid-ask spread. Bid-ask spread serves to capture information asymmetry. If a new announcement or disclosure by a breached company increases uncertainty, then the bid-ask spread will increase. Alternatively, if a new announcement/disclosure decreases uncertainty, the bid-ask spread will decrease. Much research in the accounting and finance literature confirms these findings; for example, Coller and Yohn (1997) documented that the bid-ask spread after management earnings forecasts is significantly smaller than that before the announcements. Other studies include bid-ask spread changes in response to auditor changes (Hagigi, Kluger, and Shields 1993), stock repurchases (Franz, Rao, and Tripathy 1995), bankruptcies (Frino, Jones, and Wong 2007), and mergers and acquisitions (Chan, Ge, and Lin 2015). Since a data breach announcement should be completely unexpected (Rosati et al. 2017), it is reasonable to expect that an abnormal level of spread might ensue due to information shock, which creates higher uncertainty and thus increases the risk of exposure from informed trading for focal firms.

Finally, I also use abnormal returns measures. This is a method used by many studies capturing the reaction of the market to the effect of data breaches. One exception is Rosati et al. (2017), who used abnormal turnover and abnormal bid-ask spreads to measure the reaction of the market to data breaches.

As discussed above, the effects on the markets of rivals of data breaches on the part of focal firms are not clear; thus, the following hypotheses are suggested:

H1a*: The abnormal trading volume of rival firms is significantly related to the announcement of security breaches of focal firms.*

H1b*: The abnormal bid-ask spread of rival firms is significantly related to the announcement of security breaches of focal firms.*

H1c*: The abnormal returns of rival firms are significantly related to the announcement of security breaches of focal firms.*

For trading volume, I utilize daily stock turnover. The methodology I follow for daily stock turnover is the same as that of Rosati et al. (2017) . Turnover is defined as trading volume divided by outstanding shares. I calculate the abnormal turnover as follows:

$$ATURN_{i,t} = (TURN_{i,t} - NTURN_{i,t}) / std\ (NTURN_{i,t}) \quad \text{Eq. (2.2)}$$

$$NTURN_{i,t} = \left(\sum_{-132}^{-6} TURN_{i,t}\right)/126 \quad \text{Eq. (2.3)}$$

Here, $TURN_{i,t}$ is the turnover on day t associated with event i; $ATURN_{i,t}$ is the abnormal turnover on day t associated with event i; and $NTURN_{i,t}$ is the average normal turnover associated with event i as calculated over the estimation period. The model for formal testing of the cross-sectional average abnormal turnover is:

$$\overline{ATURN_t} = 1/n \left(\sum_{i=1}^{n} ATURN_{i,t}\right),\ t = -5 \text{ to } +5 \quad \text{Eq. (2.4)}$$

I also estimate the abnormal bid-ask spread as suggested by Rosati et al. (2017). The following models are suggested for assessing the bid-ask spread:

$$ABAS_{i,t} = (BAS_{i,t} - NBAS_{i,t}) \quad \text{Eq. (2.5)}$$

$$NBAS_i = (\sum_{-132}^{-6} BAS_{i,t})/126 \quad \text{Eq. (2.6)}$$

Here, $BAS_{i,t}$ is the bid-ask spread on day t with event i; $ABAS_{i,t}$ is the abnormal bid-ask spread on day t associated with event i; and $NBAS_i$ is the average normal bid-ask spread associated with event i as calculated over the estimation period. The model for formal testing of the cross-sectional average abnormal bid-ask spread is:

$$\overline{ABAS_t} = 1/n \left(\sum_{i=1}^{n} ABAS_{i,t}\right), t = -5 \text{ to } +5 \quad \text{Eq. (2.7)}$$

Finally, I measure the reaction of market by using Cumulative Abnormal Returns (CAR). This measure is in line with previous studies that measured the reactions of the market to the announcement of data breaches of focal firms. To determine whether an announcement affects the stock price, the study first estimate what the return of the stock would have been had the event not occurred, that is, the normal return. There are several ways to calculate the normal return, such as Capital Assets Pricing Model (which is also called the market model), and the Fama-French Three Factor Model. Consistent with prior studies, I use the market model. The model is:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \quad \text{Eq. (2.8)}$$

Here $R_{i,t}$ is the return of the stock i on day t; $R_{m,t}$ is the return on the market portfolio on day t; α_i and β_i are the intercepts and slope coefficients respectively for firm i; and $\varepsilon_{i,t}$ is the disturbance term for stock i on day t, with Ordinary Least Square (OLS) properties. The event window is – five to + five days and the estimation window is – 132 to – six days. Research suggests that the estimation period typically ranges from 120 days

to 200 days (Cavusoglu, Mishra, and Raghunathan 2004). My estimation period and event period are in line with Rosati et al (2017). I obtain stock price data from the Center for Research in Security Prices database (CRSP) and financial data from the COMPUSTAT database. The equations to measure Abnormal Return (AR) and Cumulative Abnormal Return (CAR) are given below:

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i R_{m,t}) \quad \text{Eq. (2.9)}$$

$$CAR_i = \sum_{t=-T}^{T} AR_{i,t} \quad \text{Eq. (2.10)}$$

Here, $R_{i,t}$ = return of stock *i* at time *t*; $R_{m,t}$ = market return at time *t.* α_i and β_i = OLS parameter estimates obtained from estimation period.

Information Technology Governance (ITG), a subset of corporate governance, focuses on information and technology and its performance and risks. In other words, ITG is a combination of tools, processes, methodologies that help organizations align strategy and goals with IT services, infrastructure, or environments by reducing the risks arising from the use of IT. A high level of board ITG involvement has implications for strategic alignment and organizational performance (Turel and Bart 2014; Turel, Liu, and Bart 2017). Zafar, Ko, and Osei-Bryson (2016) documented that when organizations experience data breaches, organizations which have Chief Information Officers (CIO) in their top management team can recover damages or losses quicker than organizations that do not. Further, they find that having a CIO in top management has a significant positive impact on firm performance in the aftermath of data breaches. Feng and Wang (2018) study the relationship between a CIO's risk appetite and subsequent data breaches, and suggest that the CIO's risk aversion is negatively associated with the likelihood of

security incidents. Further, they confirm that this association is stronger if the Chief Executive Officer (CEO) is risk averse, as well. Higgs et al. (2016) studied the signaling effect of the existence of board-level technology committees to the firms' ability to detect and respond to security breaches. Their results indicated that firms with technology committees are more likely to have reported the occurrence of breaches in a given year than are firms without such committees; it is likely that such results arise from "young" technology committees and external sources of breaches, however. As a technology committee becomes more mature and established, a firm is not as likely to be breached. Further, Higgs et al. (2016) documents that the presence of technology committee mitigates negative market reactions arising from the data breaches. Taken together, these results suggest that strong Information Technology Governance (ITG) has implications for market reactions to data breaches.

Kwon, Ulmer, and Wang (2012) examined how an IT executive's position in a top management team and how his/her compensation are associated with the probability of data breaches. Their results indicate that an IT executive's involvement in the top management team is negatively associated with the possibility of information security breaches. They also found that the compensation differences between IT and non-IT executives are negatively associated with the likelihood of information security breaches. Haislip, Lim, and Pinsker (2017) investigated the independent relationship of CEO IT expertise, Chief Financial Officer (CFO) IT expertise, and the existence of board level technology committees with the subsequent likelihood of data breaches. Their results indicate that firms that either employ a CEO with IT expertise or implement a technology committee are more likely to detect and report breaches. However, firms that employ a

CFO with IT expertise are less likely to report a breach, thus suggesting that these firms are better at preventing breaches. Moreover, Haislip et al. (2016, 2015) document that firms experiencing Information Technology Material Weakness (ITMW) also experience higher CEO, CFO, and director turnover than non-ITMW firms; moreover, these ITMW firms hire CEOs, CFOs, and directors with higher levels of IT expertise, and upgrade their IT significantly following ITMW events as an attempt to legitimize their existence. Taken together, these findings suggest that ITG has implications for the occurrence of security breaches. Extrapolating these findings relating characteristics of focal firms to rival firms, I hypothesize the following:

H2a*: The Information Technology Governance (ITG) in rival firms is significantly associated with abnormal trading volume in response to the announcement of data breaches of focal firms.*

H2b*: Information Technology Governance (ITG) in rival firms is significantly associated with abnormal bid-ask spreads in response to the announcement of data breaches of focal firms.*

H2c*: The Information Technology Governance (ITG) in rival firms is significantly associated with abnormal returns in response to the announcement of data breaches of focal firms.*

In order to measure ITG, I adopt a holistic view. I do not confine ITG to only the technology committee; rather, I include the role of CIO, Chief Security Officer (CSO), the Risk Committee, and the Compliance Committee. Since the literature supports the role each of these high offices in cybersecurity risk management, the measurement will represent the underlying construct well. If the rival firms have any of these roles in their

executive position, they will be represented by a variable called ITG, where one presents the existence of either tech committee, risk committee, compliance committee, CIO, or CSO; 0, otherwise.

However, as suggested by Higgs et al. (2016), having a strong ITG is not a random occurrence, which suggests the potential for endogeneity issues; that is, firms having strong ITG might be more (less) likely to be breached. To address the endogeneity issue, I will use propensity score matching as was done by Higgs et al. (2016). Like Higgs et al. (2016), I will use the ITG prediction model from Premuroso and Bhattacharya (2007). The model is:

$$ITG = \gamma_0 + \gamma_1 (R\&D\ Exp) + \gamma_2 (NPM) + \gamma_3 (ROE) + \gamma_4 (LEVERAGE) + \gamma_5 (ROA) + \gamma_6 (WC) + \gamma_7 (Tobin's\ q) + \gamma_8 (LOGTA) + \gamma_9 (LOSS) + \gamma_{10} (IC\_WEAKNESS) + \gamma_{11} (PAST\_BREACH) + \varepsilon \quad \text{Eq. (2.11)}$$

Here, *R&D Exp* is research and development and in-process R&D expense reported in company income statements; *NPM*, net profit margin, is net income divided by total revenue; ROE, return on equity, is net income divided by average shareholders' equity; *LEVERAGE* is calculated as long-term debt divided by average shareholders' equity; *ROA*, return on assets, is net income divided by average assets; *WC*, working capital, is current assets divided by current liabilities; *Tobin's q* is the market value of equity divided by assets; *LOGTA* is the natural log of total assets; *LOSS* is a dummy variable equal to one if the firm reports a negative net income, zero otherwise; and *IC_WEAKNESS* is an indicator variable equal to one if the company has a material weakness in internal control over financial reporting, zero otherwise; *PAST_BREACH* is an indicator variable equal to one if the rivals have experienced a previous data breach,

zero otherwise. By using propensity score matching, I will calculate a matched sample and run the analysis for the matched sample.

Firms compete for resources and capabilities in the strategic factor markets. If two firms are strategically similar, then that similarity impacts firm behavior and shapes the competitive dynamics for the two firms. There are two schools of thought about the relationship between strategic similarity and rivalry; one school of thought, which lacks generalizability, suggests that strategic similarity between two firms reduces rivalry. The latter school of thought suggests the opposite and has a degree of empirical support (Gimeno and Woo 1996). So, if focal firms and rivals are strategically similar, then it is expected that the announcement of data breaches by focal firms will affect rivals. Feng and Wang (2018) documented that the strategic position of a company acts as a moderator in the relationship between CIO risk aversion and the occurrence of data breaches. Strategic similarity intensifies the rivalry among firms and financial markets will react per the choices made by these firms. Whenever a firm announces a data breach, it aims to procure a bundle of useful resources to create capabilities to avoid future incidents. The increased capabilities may result in higher financial performance and markets will react positively to the focal firm's improved performance and profitability. In that manner, the market is more concerned about the future cash flows associated with a firm's decision.

After the announcements of a data breach, if the focal firm becomes more competitive in the product market by deploying newly acquired resources or products, then financial markets will presume that the future cash flows of the firm will be higher and stable. At the same time, the financial markets may penalize the rivals believing that

they do not have such surety and stability in their cash flows. Moreover, if the industry in which these firms operate is a low-growth industry, then higher cash flows to the focal firms may come at the expense of existing rivals. Hence, the effect of data breach announcements on the rival firm's profitability and future cash flows can be negative and particularly larger in magnitude if the firms are strategically similar than if they are not strategically similar. The similarity of how these firms respond to different market situations and rivals' actions intensifies the rivalry among the existing firms in an industry. Strategically similar firms benefit at the expense of the remaining firms in the industry, so financial markets respond by penalizing strategically similar rivals more than strategically dissimilar rivals. Hence, strategic similarity can moderate the relationship between rivals' market valuations and a focal firm's data breach announcement. So, the following hypotheses are offered:

H3a*: The trading volume of strategically similar rival firms is significantly related to the announcement of security breaches of focal firms.*

H3b*: The bid-ask spread of strategically similar rival firms is significantly related to the announcement of security breaches of focal firms.*

H3c*: The abnormal returns of strategically similar rival firms are significantly related to the announcement of security breaches of focal firms.*

A firm's strategic emphasis can be captured using proxies from four dimensions —strategic capabilities, technological intensity, marketing intensity, and market-specific experience (Uhlenbruck et al. 2017). Hence, I will use these four dimensions to capture the strategic similarity/overlap between rivals and the focal firm. I use firm size, measured as the log of total assets, as a proxy to measure strategic capabilities,

product-market strategies, and network strength (Josefy et al. 2015). Following Lepak, Takeuchi, and Snell (2003), technological intensity was operationalized using capital intensity and Research and Development (R&D) intensity. I will divide the summation of capital expenditure (CAPEX) and R&D expenses by sales to measure technological intensity (Baysinger and Hoskisson 1989; Osborn and Baughn 1990). Marketing intensity was operationalized by dividing total marketing and advertising expenses of a firm by its sales. The final dimension, market-specific experience, is proxied as the number of years a firm has been in operation since its Initial Public Offering (IPO). The *names* database from WRDS was used to get the year in which the companies began public trading. All of the variables above were averaged for both focals and rivals. Then, strategic similarity, following the model suggested by Gimeno and Woo (1996), is measured by one minus the Euclidean distances between the points in four-dimensional space (normalized to a zero to one range). Gimeno and Woo (1996, 330) suggested the following model for strategic similarity:

$$Similarity = 1 - \frac{\sqrt{\sum_{v=1}^{4}(z_{iv}-z_{jv})^2}}{max(k,l)\sqrt{(z_{kv}-z_{lv})^2}} \qquad \text{Eq. (2.12)}$$

The measure will take the value of zero (minimum similarity) when the Euclidean distance in the strategic space between two firms is the largest for all pairs in the sample, and it equals one (maximum) when the Euclidean distance is zero (indicating that firms are equal in competitive orientation).

Research suggests that different kinds of cross sectional variations (also called contingency factors) such as business type, industry, type of breach, event year, and firm size can moderate the extent of market reactions to data breaches (Yayla and Hu 2011;

Andoh-Baidoo and Osei-Bryson 2007; Gatzlaff and McCullough 2010). Therefore, although the moderating effects of the above contingency factors are not hypothesized, I also study the extent of market reactions conditioned on some of these moderating variables. The following models are suggested for the study:

$$ATURN = \beta_0 + \beta_1 (ln\_PRC) + \beta_2 (Spread) + \beta_3 (Var_i) + \beta_4 (ln\_mktCap) + \beta_5 (BMRatio_i) + \beta_6 (Leverage) + \beta_7 (ln\_BrScale) + \beta_8 (Prior\_Breach\_Yes) + \beta_9 (BreachType) + \beta_{10} (FirmType) + \beta_{11} (ITG) + \beta_{12} (Similarity) + \varepsilon_i \quad \text{Eq. (2.13)}$$

$$ABAS = \beta_0 + \beta_1 (ln\_PRC) + \beta_2 (Turnover) + \beta_3 (Var) + \beta_4 (ln\_mktCap) + \beta_5 (BMRatio) + \beta_6 (Leverage) + \beta_7 (ln\_BrScale) + \beta_8 (Prior\_Breach\_Yes) + \beta_9 (BreachType) + \beta_{10} (FirmType) + \beta_{11} (ITG) + \beta_{12} (Similarity) + \varepsilon_i \quad \text{Eq. (2.14)}$$

$$CAR = \beta_0 + \beta_1 (FirmType) + \beta_2 (ln\_mktCap) + \beta_3 (ln\_BrScale) + \beta_4 (Prior\_Breach\_Yes) + \beta 5 (BreachType) + \beta_6 (ITG) + \beta_7 (Similarity) + \varepsilon_i \quad \text{Eq. (2.15)}$$

Here, *ATURN* = the abnormal turnover; *ABAS* = abnormal bid-ask spread; *CAR* = Cumulative Abnormal Return; *ln_PRC* = natural logarithm of the closing price and it represents dealer's ordering cost; *Turnover* = stock daily turnover and it proxies for inventory-holding cost; *Spread* = the bid-ask spread calculated using the Corwin and Schultz (2012) model[2]. *Var* = the difference between the low bid and high ask price, and it proxies for dealer's inventory-holding risks; *ln_mktCap* = natural log of market capitalization; *BMRatio* = book-to-market ratio; *Leverage* = debt-to-asset ratio; *ln_BrScale* = natural log of the number of records breached; *Prior_Breach_Yes* = dummy variable 1 = if a focal firm experienced a data breach before and zero otherwise; *BreachType* = {Active, Stolen, Lost; and Unknown}[3]; *FirmType* = 1 if financial

[2] Much research in the accounting and finance literature follows the Corwin and Schultz (2012) procedure to calculate the bid-ask spread (Cho, Lee, and Pfeiffer Jr 2013; Egginton and McCumber 2018; Rosati et al. 2017).

[3] The classification is done following Rosati et al. (2017).

companies, zero otherwise; *Similarity* = Strategic Similarity between focals and rivals calculated using Eq. 2.12.

Research Methodology

Sample

The event of interest for the study is the announcement of an information data breach. I collected the data breach event from privacyrights.org as compiled by Privacy Rights Clearing House, a California based non-profit organization. Many studies have used the same data set to identify announcement dates of data breaches (Higgs et al. 2016; Feng and Wang 2018; Rosati et al. 2017; Edwards, Hofmeyr, and Forrest 2016). For rivals (competitors) selection, I used the Text-based Network Industry Classification (TNIC) database developed by Hoberg and Phillips (2016). The focal-rival pair in the database is based on firms' product market descriptions in their annual reports (10-Ks). The literature suggests that a pair in the database is exposed to different kinds of correlated shocks (Foucault and Fresard 2014), and indicates three important features of the database: first, unlike industry-based classification such as Standard Industrial Classification (SIC) or North American Industry Classification System (NACIS), the focal-rival pairs change over time, in accordance with changes in firms' innovation, product ranges and so on; second, the pairings are based on the products that firms usually sell rather than its production processes; and third, unlike SIC and NAICS industries, TNIC industries do not require relations between firms to be transitive. Foucault and Fresard (2014, 564) suggest that these specific characteristics of the data provides " a richer definition of similarity and product market relatedness." Though I have collected data breach events for the year 2005-2017 from privacyrights.org website,

the TNIC database available data period covers 2005-2015 during the preparation of this dissertation; therefore, I excluded data breach events for the years 2016-2017.

From the privacyrights.org database I obtained 6166 data breach event dates, but many of the dates are related to non-publicly-listed companies; therefore, I have excluded the data for companies not publicly traded, as well as information about breaches in which there is no mention of the number of records lost. After merging the remaining data with CRSP, COMPUSTAT, and BOARDEX database, I identified 121 data breach events (Table 2.1) for publicly listed companies. Table 2.2 represents the distribution of the breaches by year, from which it is apparent that more than 25% data breaches occurred in the years 2013-2015. One hundred twenty-one data breach events represent 76 focal companies. Table 2.3 and Table 2.4 represent the distribution of those companies by industry and year, respectively. More than 30% of focal companies belong to the Finance, Insurance, and Real Estate industries.

When I identify all rivals for focal firms (data breached firms), I obtain about 11,500 rivals; however, following the extant literature and as suggested by Hoberg and Phillips (2016), I selected the nearest five rivals for each focal firm using the similarity score provided in the TNIC database. This process identified 589 event dates for 363 rivals[4]. As is the case for focal firms, more than 30% of rivals belong to the Finance, Insurance, and Real Estate industries.

[4] In some cases, the nearest five rivals were not available for a focal firm; therefore, the total rival events are 589, not 605 (121×5) events.

Table 2.1

Total Number of Data Breaches (2005-2015)

Total Number of data breaches (2005-2017)	6166
Less: Number of data breaches related to not-listed companies	5550
Less: Number of data breaches with zero number of records lost	281
Less: Number of data breaches related to the years 2016-2017 and missing records in COMPUSTAT, CRSP, and BOARDEX	214
Total number of data breaches	**121**

Table 2.2

Distribution of Data Breaches by Year

Year	**n**	**percent**	**cumulative**
2005	6	4.95	4.95
2006	13	10.74	15.70
2007	16	13.22	28.92
2008	10	8.26	37.19
2009	6	4.95	42.14
2010	11	9.09	51.24
2011	10	8.26	59.50
2012	9	7.43	66.94
2013	14	11.57	78.51
2014	15	12.39	90.90
2015	11	9.09	100.00
Total	**121**		

Table 2.3

Distribution of Companies by Industry

Industry	**Focals**	**Rivals**
Construction	1	5
Finance, Insurance, and Real Estate	26	116
Manufacturing	12	57
Mining	0	2
Public Administration	0	1
Retail Trade	12	52
Services	17	78
Transportation, Communications, Electric, GAS, and Sanitary Services	7	42
Wholesale Trade	1	10
Total	**76**	**363**

Table 2.4

Distribution of Companies by Year

Year	Focals	Rivals
2005	5	25
2006	10	47
2007	16	64
2008	7	40
2009	5	23
2010	6	29
2011	4	21
2012	7	35
2013	7	32
2014	5	30
2015	4	17
Total	**76**	**363**

Results

Summary Statistics

Table 2.5 presents the summary statistics between focal firms (data breached) and rival firms. The continuous variables are winsorized at 1% and 99% levels. The variable *ln_mktCap* indicates that focal firms are larger in size than rival firms (9.8 vs 8.09) and this difference is statistically significant. The *BMRatio* of rivals is greater than that of focal firms, indicating that focal firms have higher growth potential than rival firms. Additionally, there is also significant difference between focal firms and rivals in terms of closing prices of stocks. Furthermore, both focal firms and rivals are highly leveraged. No statistical tests are done on the variables *BREACH_TYPE_Active*, *BREACH_TYPE_Lost*, *BREACH_TYPE_Stolen*, *FirmType*, *ln_BrScale*, and *Prior_Breach_Yes* because they are only related to focal firms, but the sample of rival firms includes those characteristics if the focals of the rival firms have those characteristics.

Table 2.5

Summary Statistics and Tests of Differences of Focals and Rivals

	Focals						Rivals						Difference	
Statistic	**N**	**Mean**	**Std. Dev**	**Q1**	**Median**	**Q3**	**N**	**Mean**	**Std. Dev**	**Q1**	**Median**	**Q3**	**t-stat**	**Wilcoxon Z**
Var	113	1.06	1.21	0.46	0.83	1.20	545	1.02	1.53	0.38	0.68	1.17	0.68	1.71
BMRatio	101	0.23	1.79	0.22	0.40	0.59	497	0.51	0.56	0.27	0.48	0.73	-2.46 **	-2.24 **
BREACH_TYPE_Active	121	0.27	0.45	0.00	0.00	1.00	589	0.27	0.44	0.00	0.00	1.00	NA	NA
BREACH_TYPE_Lost	121	0.07	0.26	0.00	0.00	0.00	589	0.08	0.27	0.00	0.00	0.00	NA	NA
BREACH_TYPE_Stolen	121	0.22	0.42	0.00	0.00	0.00	589	0.23	0.42	0.00	0.00	0.00	NA	NA
FirmType	121	0.40	0.49	0.00	0.00	1.00	589	0.42	0.49	0.00	0.00	1.00	NA	NA
Leverage	121	0.70	0.24	0.54	0.68	0.89	584	0.67	0.26	0.49	0.69	0.88	1.47	1.16
ln_BrScale	121	8.55	3.70	6.21	8.39	11.00	589	8.54	3.73	5.99	8.39	11.00	NA	NA
ln_mktCap	101	9.80	1.75	8.50	9.86	11.13	497	8.09	2.11	6.47	8.08	9.64	8.63 ***	7.24 ***
ln_PRC	113	3.61	0.87	3.28	3.67	4.13	542	3.31	1.05	2.83	3.42	3.98	3.18 ***	3.09 ***
Prior_Breach_Yes	121	0.36	0.48	0.00	0.00	1.00	589	0.37	0.48	0.00	0.00	1.00	NA	NA
Spread	113	0.01	0.01	0.00	0.005	0.01	543	0.01	0.01	00.00	0.005	0.01	-0.36	0.15
Turnover	113	8.49	5.56	4.47	6.80	10.95	545	8.64	10.22	3.93	6.5	10.33	-0.22	-1.00

*, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.6 presents summary statistics for the group of rivals (Unmatched Sample) by ITG = 1 and ITG = 0. The mean of *CAR (-1, 0)* of rivals with ITG = 1 is -0.001 and the mean of CAR *(-1, 0)* of rivals with ITG = 0 is 0.003; the difference is statistically significant. This suggests that the markets of rivals with ITG = 1 react negatively to breach announcements, while the markets of rivals with ITG = 0 react positively. However, the median of *CAR (-1, 0)* for both groups is negative, yet the market reaction of rivals with ITG = 1 is more negative (-0.003 vs -0.001). Together, these findings from CAR suggest that abnormal return of rivals with ITG = 1 reacts more negatively. However, the mean of *ATURN (-1, 0)* of rivals with ITG = 1 is greater than that of rivals with ITG =0 (0.27 vs .08). The same is true for the median *ATURN (-1, 0)*. For *ABAS (-1, 0),* where the mean of rivals with ITG = 1 is greater than that of rivals with ITG = 0. There is a difference in *Var* between the two groups of rivals, but it is not statistically significant. The difference of *BMRatio* is statistically significant, noting that rivals with ITG = 0 having higher growth potential. Though there is no statistically significant difference between two groups for *BREACH_TYPE_Active* and *BREACH_TYPE_Lost*, there is a statistically significant difference in *BREACH_TYPE_Stolen*; 18% of rivals with ITG = 1 experienced *BREACH_TYPE_Stolen* whereas 25% of rivals with ITG = 0 experienced *BREACH_TYPE_Stolen*. It was also noted that 57% of rivals with ITG = 1 belong to the finance and insurance industries, and this group of rivals is also more heavily leveraged.

It was found that 36% of rivals with ITG = 0 belong to the same industry. Additionally, the breach scale (*ln_BrScale*) of the rivals with ITG = 1 is less than that of rivals with ITG = 0. Rival firms with ITG = 1 are larger than rival firms with ITG = 0, as

well. Further, there are statistically significant differences between the two groups (0.49 vs 0.31) in terms of *Prior_Breach_Yes*. Overall, these figures suggest that there are significant differences between the rivals with ITG = 1 and rivals with ITG = 0.

Table 2.7 presents summary statistics of rivals (Propensity Score Matched Sample) by ITG = 1 and ITG = 0. As expected, it is evident that the variables used in Eq. 2.11 are not statistically significant between the two groups of rivals. Only *ATURN (-1, 0)* is statistically significant, rivals with ITG = 1 having higher abnormal turnover than the rivals with ITG = 0. Moreover, *ABAS (-1, 0)* of rivals with ITG = 1 is smaller than that of rivals with ITG = 0. Similarly, *CAR (-1, 0)* of rivals with ITG = 1 is positive, with the *CAR (-1, 0)* of rivals with ITG = 0 being negative. Also, *ln_BrScale* of rivals with ITG = 1 is greater than that of rivals with ITG = 0. The same is true for *Prior_Breach_Yes*. Taken together, the findings suggest that though rivals with ITG = 1 are more susceptible to frequent and large data breaches, markets have positive reactions to the data breaches of focal firms.

Table 2.6

Summary Statistics and Tests of Differences of Rivals (Unmatched Sample)

	ITG												
	1						0						
Statistic	**N**	**Mean**	**St. Dev.**	**Q1**	**Median**	**Q3**	**N**	**Mean**	**St. Dev.**	**Q1**	**Median**	**Q3**	**t-test/ χ^2**
ATURN (-1,0)	185	0.27	1.91	-0.87	0.03	0.90	363	0.08	2.00	-0.98	-0.36	0.59	-1.05
ABAS (-1,0)	184	0.002	0.01	-0.01	-0.001	0.01	361	0.001	0.02	-0.01	-0.002	0.01	-0.34
CAR (-1,0)	184	-0.001	0.03	-0.01	-0.003	0.01	360	0.003	0.04	-0.01	-0.001	0.02	1.64 *
Var	185	0.96	0.95	0.39	0.68	1.14	363	1.05	1.75	0.37	0.68	1.18	0.80
BMRatio	166	0.62	0.41	0.35	0.58	0.83	334	0.45	0.61	0.26	0.43	0.66	-3.77 ***
BREACH_TYPE_Active	191	0.27	0.45	0.00	0.00	1.00	398	0.26	0.44	0.00	0.00	1.00	0.014
BREACH_TYPE_Lost	191	0.09	0.29	0.00	0.00	0.00	398	0.07	0.25	0.00	0.00	0.00	0.93
BREACH_TYPE_Stolen	191	0.18	0.38	0.00	0.00	0.00	398	0.25	0.44	0.00	0.00	1.00	3.78 *
FirmType	191	0.57	0.50	0.00	1.00	1.00	398	0.36	0.48	0.00	0.00	1.00	22.16 ***
Leverage	191	0.74	0.22	0.60	0.84	0.90	396	0.63	0.27	0.44	0.62	0.83	-5.21 ***
ln_BrScale	191	8.17	3.52	6.29	7.76	10.52	398	8.72	3.81	5.92	8.76	11.08	1.73 *
ln_mktCap	166	8.75	2.04	7.59	8.96	10.40	334	7.74	2.07	6.25	7.62	9.41	-5.19 ***
ln_PRC	184	3.39	0.89	2.90	3.46	3.95	361	3.27	1.12	2.73	3.38	4.01	-1.30
Prior_Breach_Yes	191	0.49	0.50	0.00	0.00	1.00	398	0.31	0.46	0.00	0.00	1.00	16.77 ***
Spread	185	0.01	0.01	0.00	0.004	0.01	361	0.01	0.01	0.00	0.01	0.01	1.65 *
Turnover	185	8.20	6.07	4.29	6.75	10.79	360	8.86	11.80	3.44	6.31	10.12	0.86

*, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.7

Summary Statistics and Tests of Differences of Rivals (Matched Sample)

	ITG												
	1						0						
Statistic	**N**	**Mean**	**St. Dev.**	**Q1**	**Median**	**Q3**	**N**	**Mean**	**St. Dev.**	**Q1**	**Median**	**Q3**	**t-test/χ2**
R&D Exp	29	5.35	2.29	3.28	5.63	7.04	29	4.82	1.90	3.28	5.53	6.12	-0.96
NPM	29	0.07	0.12	0.03	0.06	0.11	29	0.05	0.11	0.03	0.05	0.08	-0.76
ROE	29	0.18	0.19	0.12	0.20	0.29	29	0.17	0.41	0.08	0.13	0.20	-0.20
ROA	29	0.06	0.08	0.04	0.07	0.09	29	0.05	0.07	0.02	0.04	0.08	-0.51
WC	29	1.90	1.08	1.11	1.69	2.27	29	1.88	1.30	1.12	1.55	2.18	-0.05
Tobin's q	29	1.65	1.08	1.09	1.37	2.00	29	1.31	0.97	0.77	1.00	1.62	-1.28
LOGTA	29	8.62	2.11	6.76	8.56	10.25	29	8.24	1.98	6.55	8.28	9.52	-0.70
LOSS	29	0.10	0.31	0.00	0.00	0.00	29	0.10	0.31	0.00	0.00	0.00	0.00
IC_WEAKNESS	29	0.00	0.00	0.00	0.00	0.00	29	0.00	0.00	0.00	0.00	0.00	0.00
PAST_BREACH	29	0.03	0.19	0.00	0.00	0.00	29	0.00	0.00	0.00	0.00	0.00	0.00
ATURN (-1,0)	29	0.88	2.35	-0.55	0.61	1.67	29	-0.20	1.55	-1.11	-0.56	0.59	-2.07**
ABAS (-1,0)	29	-0.001	0.01	-0.01	-0.001	0.01	29	0.0001	0.01	-0.01	-0.0002	0.005	0.17
CAR (-1,0)	29	0.0004	0.03	-0.01	0.003	0.01	29	-0.002	0.02	-0.01	-0.004	0.01	-0.41
Var	29	1.22	1.36	0.36	0.63	1.41	29	1.12	0.84	0.42	0.96	1.60	-0.33
BMRatio	29	0.31	0.18	0.18	0.29	0.44	29	0.37	0.26	0.23	0.29	0.50	1.04
BREACH_TYPE_Active	29	0.17	0.38	0.00	0.00	0.00	29	0.17	0.38	0.00	0.00	0.00	0.00
BREACH_TYPE_Lost	29	0.03	0.19	0.00	0.00	0.00	29	0.10	0.31	0.00	0.00	0.00	0.27
BREACH_TYPE_Stolen	29	0.52	0.51	0.00	1.00	1.00	29	0.55	0.51	0.00	1.00	1.00	0.00
FirmType	29	0.03	0.19	0.00	0.00	0.00	29	0.03	0.19	0.00	0.00	0.00	0.00
Leverage	29	0.56	0.22	0.41	0.58	0.76	29	0.59	0.20	0.46	0.62	0.76	0.45
ln_BrScale	29	9.40	3.38	6.64	9.74	12.24	29	8.29	3.14	5.69	7.08	11.00	-1.30
ln_mktCap	29	8.91	2.13	7.27	9.58	10.85	29	8.31	1.77	6.89	8.28	9.17	-1.17
ln_PRC	29	3.48	1.22	2.96	3.42	4.40	29	3.66	0.88	3.20	3.78	4.33	0.63
Prior_Breach_Yes	29	0.31	0.47	0.00	0.00	1.00	29	0.21	0.41	0.00	0.00	0.00	0.36
Spread	29	0.01	0.01	0.0002	0.004	0.01	29	0.01	0.01	0.00	0.001	0.01	-0.04
Turnover	29	7.84	5.02	4.29	6.81	8.80	29	7.86	3.71	5.80	7.35	8.84	0.02

*, **, *** significance at 10, 5 and 1% levels respectively.

Correlation Matrix

Table 2.8 is the correlation matrix of the variables used for the study. *ATURN (-1, 0)* has statistically significant correlations with some of the control variables, such as *Var*, *ln_mktCap,* and *Leverage*. As expected, both *ATURN (-1, 0)* and *ATURN (-1, +1)* have a statistically significant negative correlation with *BREACH_TYPE_Active*. This suggests that when focal firms' data breach types are "active," then their rivals' abnormal turnover goes down. *ABAS (-1, 0)* has also significant negative correlations with the control variables. Further, *ABAS (-1, 0)* has a significant negative correlation with *BREACH_TYPE_Stolen*, which is unexpected; however, *ABAS (-1,+1)* has a significant positive relationship with *Prior_Breach_Yes,* suggesting that when focal firms have a history of data breaches, their rival firms also experience uncertainty in their information environment.

CAR (-1, 0) is significantly negatively correlated with the data breaches scale (*ln_BrScale*) and data breach type (*BREACH_TYPE_Lost*). *CAR (-1, +1)* is also significantly negatively correlated with both *ln_BrScale* and *BREACH_TYPE_Active*. *ITG* is significantly and positively correlated with *ln_mktCap*, *BMRatio*, *Leverage*, *FirmType*, *Prior_Breach_Yes*, but negatively correlated with *BREACH_TYPE_Stolen*. These suggest that large organizations, high growth potential companies, highly leveraged firms, or firms belonging to the finance or insurance industries are more likely to have *ITG,* which consists of a technology committee, a CIO, Chief Security Officer, a risk committee or a compliance committee. As shown above, the data breach history of focal firms and the characteristics of their breaches are correlated with *ITG*.

Table 2.8

Correlation Matrix

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1. ln_PRC																				
2.Var	**0.78*****																			
3.Spread	**-0.09***	**-0.05**																		
4.ln_mktCap	**0.63*****	**0.47*****	**-0.07**																	
5.BMRatio	**-0.21*****	**-0.19*****	**0.07**	**-0.17*****																
6.Leverage	**0.04**	**-0.02**	**0.08**	**0.11***	**-0.02**															
7.FirmType	**0.09***	**0.07**	**0.03**	**0.02**	**0.46*****	**0.40*****														
8.ln_BrScale	**0.02**	**0.06**	**0.01**	**-0.04**	**-0.02**	**-0.18*****	**-0.09***													
9.Prior_Breach_Yes	**0.17*****	**0.12****	**0.03**	**0.19*****	**0.10***	**0.14*****	**0.14*****	**-0.06**												
10.BREACH_TYPE_Active	**-0.01**	**-0.02**	**0.06**	**0.03**	**0.08**	**0.01**	**0.04**	**0.16*****	**0.01**											
11.BREACH_TYPE_Stolen	**-0.09***	**-0.03**	**-0.06**	**-0.13****	**-0.09**	**-0.06**	**-0.16*****	**0.00**	**-0.21*****	**-0.33*****										
12.BREACH_TYPE_Lost	**-0.06**	**-0.04**	**0.03**	**-0.10***	**0.11***	**0.04**	**0.08**	**0.17*****	**-0.22*****	**-0.17*****	**-0.16*****									
13.Turnover	**0.05**	**0.26*****	**0.00**	**0.21*****	**-0.22*****	**-0.03**	**-0.19*****	**0.04**	**0.01**	**0.05**	**-0.08**	**-0.04**								
14.ATURN (-1, 0)	**0.05**	**0.17*****	**0.02**	**0.10***	**-0.06**	**0.10***	**0.00**	**0.03**	**0.06**	**-0.08***	**-0.01**	**0.04**	**0.32*****							
15.ATURN (-1, +1)	**0.03**	**0.15*****	**0.01**	**0.09***	**-0.05**	**0.09***	**0.01**	**0.06**	**0.03**	**-0.10***	**0.04**	**0.02**	**0.27*****	**0.93*****						
16.ABAS (-1, 0)	**0.09***	**0.15*****	**0.59*****	**0.12****	**-0.02**	**0.09***	**0.04**	**-0.03**	**0.08**	**0.05**	**-0.14****	**0.08**	**0.07**	**0.11****	**0.08**					
17.ABAS (-1, +1)	**0.10***	**0.15*****	**0.56*****	**0.09***	**-0.00**	**0.05**	**0.00**	**-0.03**	**0.09***	**0.06**	**-0.08**	**0.02**	**0.05**	**0.08**	**0.03**	**0.85*****				
18.CAR (-1, 0)	**0.03**	**0.09***	**0.12****	**0.02**	**0.04**	**-0.03**	**0.00**	**-0.12****	**-0.01**	**-0.08**	**0.10***	**-0.11****	**0.07**	**0.12****	**0.10***	**0.06**	**0.07**			
19.CAR (-1, +1)	**0.06**	**0.09***	**0.05**	**0.03**	**0.01**	**-0.00**	**-0.03**	**-0.13****	**0.00**	**-0.13****	**0.10***	**-0.12****	**0.04**	**0.13****	**0.13****	**0.03**	**0.04**	**0.81*****		
20.ITG	**0.03**	**0.01**	**-0.06**	**0.23*****	**0.18*****	**0.22*****	**0.20*****	**-0.05**	**0.17*****	**0.01**	**-0.08***	**0.05**	**0.05**	**0.07**	**0.05**	**0.02**	**0.01**	**-0.07**	**-0.02**	
21.Similarity	**0.10***	**0.10***	**0.02**	**0.18*****	**-0.07**	**-0.01**	**0.03**	**0.07**	**-0.03**	**-0.01**	**-0.03**	**0.04**	**0.09***	**-0.00**	**-0.01**	**0.08**	**0.03**	**-0.03**	**-0.03**	**0.01**

Abnormal Turnover (ATURN)

Table 2.9 presents the results of abnormal turnover (*ATURN*) during the event windows (-5, 5). It is evident that though the markets for focal firms react at -two day, the markets of rival firms react at -three day. However, the markets for both and focal firms react at -1 day. It is also evident that at both -two and -one days, the abnormal turnover for focal firms is negative, whereas for rival's firms it is positive. This indicates that the reaction of the rivals' market is opposite to that of focal firms' markets, which lends support to the competitive theory hypothesis. These findings are in line with Jeong, Lee, and Lim (2018), but contradict Martin, Borah, and Palmatier (2017) and Kashmiri, Nicol, and Hsu (2017). Nevertheless, no significant market reaction is documented at zero day for both focal firms and rivals. This finding is not unexpected, since prior research (Higgs et al. 2016) also did not document any market reaction for focals at zero day.

Table 2.10 presents cumulative abnormal turnover for both focals and rivals. Focal firms' turnover of stock goes down 20% and 22% during the event window (-1, 0) and (-1, 1) respectively. In contrast, rival firms' turnover of stock goes up by 12% and 16% during the same event window. These findings further confirm the competitive effect hypothesis. Though the overall market reacts positively for rival firms, Table 2.11 shows that when focal firms experience active types of data breaches (*BREACH_TYPE_Active*), the markets of rival firms react negatively. These suggest that market reactions of rival firms are conditioned on contingency factors.

Table 2.9

Abnormal Turnover of Focals and Rivals During Event Windows

Focals			Rivals		
Day	**ATURN**	**p-Value**	**Day**	**ATURN**	**p-Value**
-5	0.001	0.990	-5	0.112	0.114
-4	-0.096	0.185	-4	-0.032	0.414
-3	0.001	0.991	-3	0.125	0.026 **
-2	-0.205	0.003 ***	-2	0.096	0.064 *
-1	-0.127	0.062 *	-1	0.119	0.035 **
0	-0.066	0.333	0	0.014	0.756
1	0.005	0.968	1	0.079	0.238
2	-0.037	0.734	2	0.055	0.347
3	0.104	0.392	3	0.083	0.097 **
4	0.235	0.070 *	4	0.125	0.019 **
5	0.051	0.652	5	0.112	0.051 *

This table reports the daily average abnormal stock turnover (ATURN), along with the *p*-values associated with the t-tests on their significance (H0: ATURN = 0). *, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.10

Cumulative Abnormal Turnover of Focals and Rivals

Focals				Rivals			
Event Window	**ATURN**	***t*-value**	***p*-value**	**Event Window**	**ATURN**	***t*-value**	***p*-value**
(-1,0)	-0.20	-1.78	0.04**	(-1,0)	0.12	1.52	0.06 *
(-1,1)	-0.22	-1.26	0.10*	(-1,1)	0.16	1.57	0.06 *

This table reports the Abnormal Stock Turnover (ATURN) along with the t-values and associated p values, with the Ha: ATURN<0, for Focal firms and Ha: ATURN>0, for Rival Firms. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.11

Cumulative Abnormal Turnover of Rivals by BREACH_TYPE_Active

Event Window (-1,0) - Rivals			
BREACH_TYPE_Active	**ATURN**	***t*-value**	***p*-value**
0	0.21	2.17	0.02 **
1	-0.16		

This table reports the Abnormal Stock Turnover (ATURN) of Rivals along with the t-values and associated p values for the variable Breach_Type_Active, with the Ha: Diff (ATURN) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.12 presents regression results for abnormal turnover. The use of the cumulative event window *ATURN (-1, 0)* for multivariate analysis is in line with previous research (Martin, Borah, and Palmatier 2017). Model (1) includes the control variables related to *ATURN (-1, 0)* and *ln_PRC* and *Var* are significant, which is consistent with the findings of Rosati et al. (2017). Models 4 through 7 show that when focal firms experience active data breaches (*BREACH_TYPE_Active*), markets for the rivals react negatively (β = *-0.94, p < 0.00*). For the "stolen" breach type (*BREACH_TYPE_Stolen*), markets also react negatively, but the effect is not statistically significant. These results suggest that there is an information transfer to the market of rival firms when the news of focal firms' data breach events arrives at markets. Although no effect of *ITG* is documented, the variable *ITG_Active* (the interaction term between *ITG* and *BREACH_TYPE_Active*) is significant and positive (β *= 1.05, p<0.00*). These findings suggest that when focal firms announce active data breach events, rivals with *ITG = 1* did not experience negative abnormal turnover. This finding also highlights the importance of strong information technology governance in remediation of data breaches. The variable *Similarity* is not significant; thus, the hypothesis that rivals who are strategically similar to focal firms will experience similar (opposite) effects in the market is not supported. I suspect this is because of the rival selection procedure using the TNIC database, which identifies rivals based on product market similarity.

Since the decision to have a technology committee, a CIO, a Chief Security Officer, a risk committee, or a compliance committee is not random, I use propensity score matching to address the endogeneity issue. When I matched the samples using Eq. 2.11, I found 58 observations (29 ITG = 1, and 29 ITG = 0). I then performed two-way ANOVA, with the two factors being *ITG* and *BREACH_TYPE_Active* or *BREACH_TYPE_Lost*, or

Prior_Breach_Yes. Figure 2.2 compares the unmatched sample and matched sample two-way ANOVA results. It is evident from Figure 2.2 (a), produced from an unmatched sample, that *ATURN (-1, 0)* is less when *BREACH_TYPE_Active* = 1 and *ITG* = 0, than when *BREACH_TYPE_Active* = 0 and *ITG* =0. However, the presence of *ITG = 1*, pulls up *ATURN (-1, 0)*, suggesting that strong information technology governance has a positive effect on *ATURN (-1, 0)*. For the matched sample (Figure 2.2 (b)), the same effect is also evident. In Figure 2.2 (c) and Figure 2.2 (e), the effect of ITG is not evident; however, it is clear from Figure 2.2 (d) and Figure 2.2 (f) that *ITG* has a positive effect on abnormal turnover (*ATURN (-1, 0)*). Overall, these findings suggest that strong information technology governance of rival firms has some shielding effects when focal firms experience data breaches. Table 2.13 is the regression analysis for the propensity score matched sample. The results suggest that when focal firms have a history of data breaches (*Prior_Breach_Yes*), the markets of rival firms react negatively ($\beta = -1.56, p<0.06$). The same is also true for "lost" (*BREACH_TYPE_Lost*) data breaches ($\beta = -1.56, p<0.10$). However, when there is strong *ITG* in rival firms, then markets react positively ($\beta = 1.37, p<0.08$). Together, these findings suggest that the characteristics of data breaches of focal firms have a negative effect on the turnover of stock, but that strong *ITG* plays a shielding role in mitigating those negative effects.

Table 2.12

Regression Analysis for ATURN (Unmatched Sample)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	ATURN (-1,0)	**ATURN (-1,0)**	**ATURN (-1,0)**	**ATURN (-1,0)**	**ATURN (-1,0)**	**ATURN (-1,0)**	**ATURN (-1,0)**
ln_PRC	-0.25**	-0.25*	-0.26**	-0.29**	-0.28**	-0.28**	-0.28**
	(0.01)	(0.06)	(0.04)	(0.03)	(0.04)	(0.04)	(0.03)
Var	0.51****	0.63****	0.63****	0.63****	0.62****	0.64****	0.65****
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
Spread	8.20	3.39	2.88	3.79	5.82	5.36	4.61
	(0.23)	(0.65)	(0.70)	(0.61)	(0.49)	(0.51)	(0.54)
In_mktCap		0.014	0.0023	0.012	-0.0084	-0.0068	-0.01227
		(0.78)	(0.96)	(0.81)	(0.87)	(0.89)	(0.82)
BMRatio		0.17	0.090	0.10	-0.066	-0.086	-0.067
		(0.55)	(0.75)	(0.71)	(0.79)	(0.72)	(0.76)
Leverage		0.60	0.52	0.52	0.75*	0.74*	0.78*
		(0.12)	(0.19)	(0.19)	(0.07)	(0.07)	(0.05)
FirmType		-0.024	-0.018	-0.021	-0.11	-0.11	-0.10
		(0.91)	(0.93)	(0.92)	(0.55)	(0.54)	(0.64)
ln_BrScale			0.0077	0.013	0.0056	0.0073	0.012
			(0.73)	(0.57)	(0.80)	(0.74)	(0.61)
Prior_Breach_Yes			**0.30***	0.27	0.26	0.18	0.17
			(0.09)	(0.14)	(0.16)	(0.33)	(0.37)
BREACH_TYPE_Active				**-0.53*****	**-0.53*****	**-0.93********	**-0.94********
				(0.01)	**(0.00)**	**(0.00)**	(0.00)
BREACH_TYPE_Stolen				-0.30	-0.15	-0.20	-0.23
				(0.16)	(0.51)	(0.38)	(0.29)
BREACH_TYPE_Lost				0.084	-0.025	-0.047	0.017
				(0.79)	(0.94)	(0.89)	(0.96)
ITG					0.23	-0.042	-0.020
					(0.22)	(0.85)	(0.93)
ITG_Active						**1.05*****	**1.004*****
						(0.00)	**(0.00)**
Similarity							0.012
							(0.96)
Cons	0.39	-0.25	-0.18	-0.013	0.056	0.18	0.17
	(0.19)	(0.59)	(0.72)	(0.98)	(0.92)	(0.74)	(0.74)
N	543	453	453	453	475	475	466
adj. R-sq	0.048	0.070	0.072	0.085	0.079	0.092	0.092

p-values in parentheses: * p<.10 ** p<.05 *** p<.01 **** p<.001

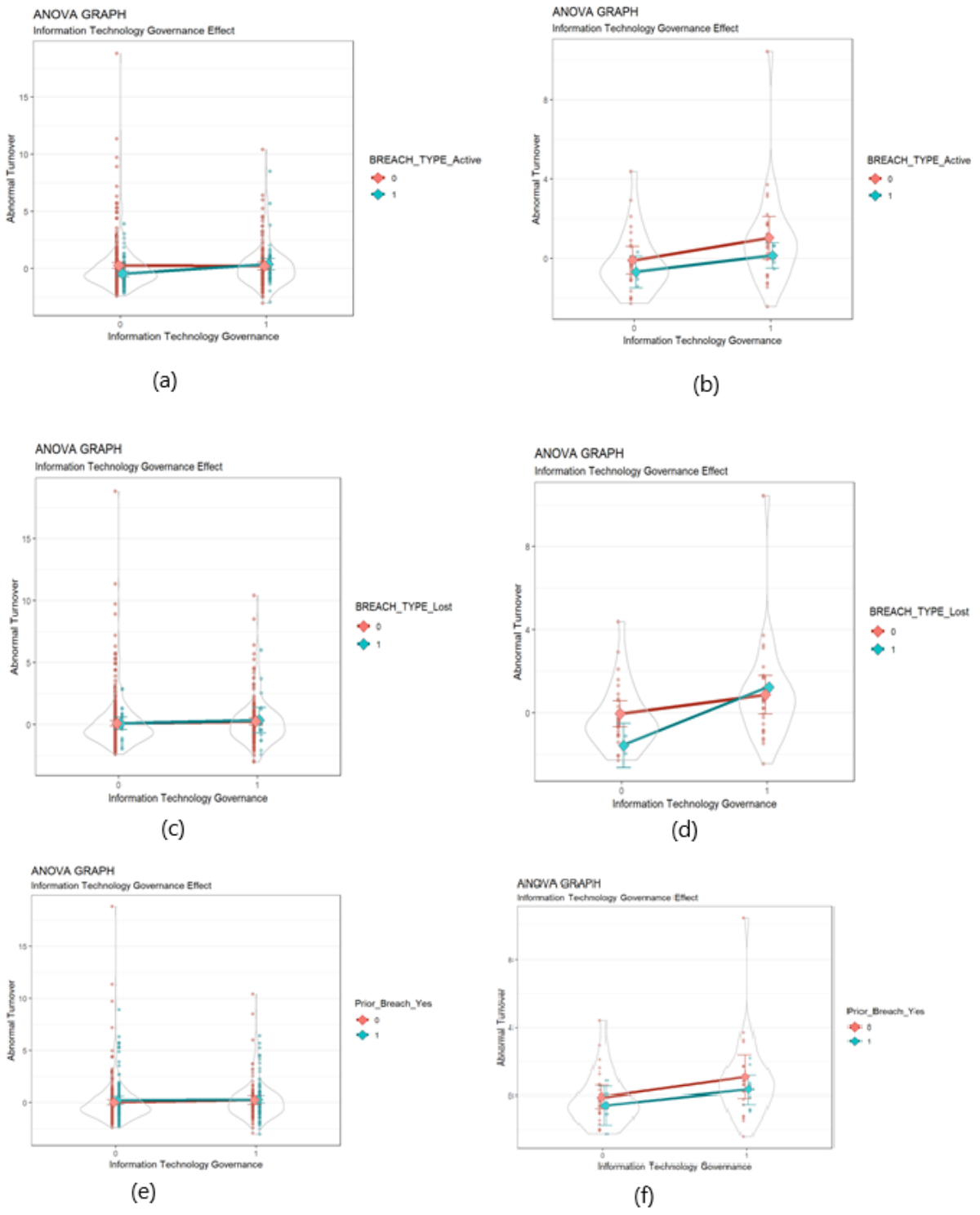


Figure 2.2 *Two-way ANOVA - Unmatched Sample (a, c, e) and Matched Sample (b, d, f)*

Table 2.13

Regression Analysis for ATURN (Matched Sample)

	(1)	(2)
	ATURN (-1,0)	**ATURN (-1,0)**
ln_PRC	0.36	0.34
	(0.60)	(0.63)
Var	0.45	0.45
	(0.21)	(0.22)
Spread	-57.9**	-57.4**
	(0.03)	(0.03)
In_mktCap	0.081	0.093
	(0.69)	(0.65)
BMRatio	2.64*	2.72*
	(0.05)	(0.06)
Leverage	1.68	1.78
	(0.20)	(0.19)
FirmType	0.33	0.44
	(0.61)	(0.53)
ln_BrScale	-0.048	-0.043
	(0.59)	(0.63)
Prior_Breach_Yes	**-1.56***	**-1.55***
	(0.06)	**(0.06)**
BREACH_TYPE_Active	-0.98	-0.82
	(0.21)	(0.37)
BREACH_TYPE_Stolen	0.16	0.17
	(0.77)	(0.76)
BREACH_TYPE_Lost	**-1.56***	**-1.58***
	(0.10)	(0.09)
ITG	**1.37***	**1.42***
	(0.08)	**(0.09)**
ITG_Active		-0.31
		(0.74)
Cons	-3.34**	-3.54**
	(0.02)	(0.02)
N	58	58
adj. R-sq	0.240	0.223

p-values in parentheses: * p<.10 **p<.05 *** p<.01 **** p<.001

Abnormal Bid-Ask Spread (ABAS)

Table 2.14 is the Abnormal Bid-Ask Spread (*ABAS*) during event windows (-5, 5) for both focal firms and rivals. As with *ATURN*, the markets of both focal and rival firms react before the release of the data breach news. However, the markets for rivals react at – three to – 1 days. At – two day, the *ABAS* of both focals and rivals is significant, but the *ABAS* of focals is higher than that of rivals (0.0017 vs 0.0009), suggesting that data breaches result in more uncertainty in focal markets than in rival markets. Table 2.15 presents the cumulative *ABAS*. The results displayed in the table suggest that cumulative *ABAS (-1, 0* and *-1, 1)* of rivals increased significantly. However, the cumulative *ABAS (-1, 1)* is significant for focal firms. Table 2.16 compares *ABAS (-1, 0)* of rival firms by *Prior_Breach_Yes* (the previous data breach history of focals). When focal firms have a previous data breach history, their rivals' *ABAS (-1, 0)* increases compared to the rivals whose focal firms did not have a previous data breach history ($t = -2.54, p<0.01$). These suggest that uncertainty goes up in rival markets where focal firms have data breach histories. Table 2.17 compares the *ABAS (-1, 0)* of rivals by *BREACH_TYPE_Lost*. When focal firms experience lost data breaches (*BREACH_TYPE_Lost*), the markets of rivals experience more uncertainty ($t = -1.68, p <0.10$) compared to when *BREACH_TYPE_Lost*= 0. These findings suggest that characteristics of the data breaches of focal firms have implications for *ABAS (-1, 0)* of rival firms.

Table 2.14

Abnormal Bid-Ask Spread of Focals and Rivals During Event Window

Focals			Rivals		
Day	**ABAS**	**p-Value**	**Day**	**ABAS**	**p-Value**
-5	0.0009029	0.1241	-5	0.0000594	0.4433
-4	-0.0008305	0.8955	-4	0.0001601	0.3389
-3	0.0007023	0.1596	-3	0.0008855	0.0176 **
-2	0.0016851	0.0321 **	-2	0.0008624	0.0316 **
-1	0.0000040	0.5021	-1	0.0013672	0.0023 ***
0	0.0008645	0.1442	0	-0.0002472	0.7114
1	0.0010711	0.0954 *	1	0.0004827	0.1273
2	-0.0000549	0.5288	2	0.0007641	0.0493 **
3	0.0000801	0.4626	3	0.0004215	0.1605
4	0.0002478	0.3776	4	0.0008265	0.0323 **
5	0.0010665	0.1205	5	0.001485	0.0003 ***

This table reports the daily average abnormal bid-ask spread (ABAS), along with the *p*-values associated with the t-tests on their significance (H0: ABAS > 0). *, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.15

Cumulative Abnormal Bid-Ask Spread of Focals and Rivals

Focals				Rivals			
Event Window	**ABAS**	***t*-value**	***p*-value**	**Event Window**	**ABAS**	***t*-value**	***p*-value**
(-1,0)	0.001210	0.92	0.18	(-1,0)	0.001376	2.02	0.02 **
(-1,1)	0.002685	1.36	0.09 *	(-1,1)	0.002073	2.37	0.00 ***

This table reports the average abnormal bid-ask spread (ABAS), along with the *p*-values associated with the t-tests on their significance (H0: ABAS > 0). *, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.16

Cumulative Abnormal Bid-Ask Spread of Rivals by Prior_Breach_Yes

Event Window (-1,0) – Rivals			
Prior_Breach_Yes	**ABAS**	***t*-value**	***p*-value**
0	0.0000361	-2.54	0.01 ***
1	0.0035988		

This table reports the Abnormal Bid-Ask Spread (ABAS) along with the t-values and associated p values for the variable Prior_Breach_Yes, with the Ha: Diff (ABAS) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.17

Cumulative Abnormal Bid-Ask Spread of Rivals by BREACH_TYPE_Lost

Event Window (-1,0) – Rivals			
BREACH_TYPE_Lost	**ABAS**	***t*-value**	***p*-value**
0	0.0010492	-1.68	0.10 *
1	0.0050991		

This table reports the Abnormal Bid-Ask Spread (ABAS) along with the t-values and associated p values for the variable BREACH_TYPE_Lost, with the Ha: Diff (ABAS) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.18 presents the multivariate regression result of *ABAS (-1, 0)*. The results confirm the above findings that focal firms' previous data breach histories (*Prior_Breach_Yes*) results in more uncertainty in rivals' market ($\beta = 0.0035, p<0.044$). Further, characteristics of the breach type (*BREACH_TYPE_Lost*) also result in market uncertainty in rivals' markets ($\beta = 0.0066, p<0.08$). Additionally, though *ITG* mitigates the market uncertainty arising from of focal firms' data breaches (- sign), it is not significant. As is the case with *ATURN (-1, 0), Similarity* is not significant. As was the case earlier, I suspect that this is because of the rival selection procedure using the TNIC database, which identifies rivals based on product market similarity. To address the endogeneity issue of *ITG*, I have used propensity scores to match samples. Figure 2.3 compares the matched and unmatched samples based on a two-way ANOVA. Figure 2.3 (a), (c), and (e) suggest that *BREACH_TYPE_Active*, *BREACH_TYPE_Lost* and *Prior_Breach_Yes* result in more uncertainty in rivals' markets as their *ABAS (-1, 0)* is greater as compared to lesser. However, Figure 2.3 (b) and (d) suggest that *ITG* helps to mitigate the market uncertainty that arises from data breaches of focal firms because when *ITG* = 1 and *BREACH_TYPE_Active* = 1, rivals' *ABAS (-1, 0)* is lesser rather than greater. The same is also true for *BREACH_TYPE_Lost*. However, for *Prior_Breach_Yes*, market uncertainty goes up when

ITG = 1. These findings might suggest that the repeated history of data breaches for focal firms can result in uncertainty in rivals' market.

Table 2.19 presents the regression results of the propensity score matched sample. The results further confirm that data breach characteristics (*BREACH_TYPE_Lost*) have significant effects ($\beta = 0.019, p < 0.03$) on *ABAS (- 1, 0)*. Further, although ITG is not significant, the interaction term *ITG_Lost* is significant, suggesting that when focal firms experience data breaches (*BREACH_TYPE_Lost*), strong information technology governance (*ITG* = 1) in rival firms helps to mitigate market uncertainty ($\beta = -0.025, p < 0.04$). Taken together, these findings suggest that focal firms' histories of data breaches and the characteristics of their data breaches result in uncertainty in rivals' markets, but that strong information technology governance in rival firms plays a mitigating role in reducing those uncertainties.

Table 2.18

Regression Analysis for ABAS (Unmatched Sample)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	ABAS (-1,0)	**ABAS (-1,0)**	**ABAS (-1,0)**	**ABAS (-1,0)**	**ABAS (-1,0)**	**ABAS (-1,0)**	**ABAS (-1,0)**
ln_PRC	0.0013	-0.000063	-0.000073	-0.00013	-0.00015	-0.00015	-0.00019
	(0.15)	(0.96)	(0.95)	(0.91)	(0.92)	(0.92)	(0.87)
Var	0.00011	0.0011	0.0011	0.0011	0.0012	0.0011	0.0011
	(0.90)	(0.32)	(0.30)	(0.28)	(0.36)	(0.36)	(0.28)
Turnover	0.00023**	0.00016	0.00016	0.00015	0.00014	0.00014	0.00014
	(0.01)	(0.11)	(0.12)	(0.13)	(0.30)	(0.31)	(0.16)
In_mktCap		0.00042	0.00031	0.00032	0.00032	0.00033	0.00033
		(0.38)	(0.52)	(0.51)	(0.52)	(0.51)	(0.52)
BMRatio		-0.00085	-0.0013	-0.0018	-0.0018	-0.0018	-0.0013
		(0.67)	(0.51)	(0.37)	(0.48)	(0.49)	(0.51)
Leverage		**0.0084****	**0.0068***	0.0058	**0.0061***	**0.0062***	**0.0063***
		(0.02)	**(0.05)**	(0.10)	**(0.10)**	**(0.09)**	**(0.08)**
FirmType		0.0012	0.0012	0.00073	0.00089	0.00083	0.0005
		(0.55)	(0.54)	(0.71)	(0.64)	(0.67)	(0.80)
ln_BrScale			-0.00019	-0.00032	-0.00029	-0.00029	-0.0003
			(0.36)	(0.13)	(0.17)	(0.17)	(0.14)
Prior_Breach_Yes			0.0026	**0.0033***	**0.0034***	**0.0035***	**0.0035***
			(0.12)	(0.05)	(0.07)	(0.06)	(0.044)
BREACH_TYPE_Active				0.0011	0.00093	0.00093	0.0012
				(0.56)	(0.61)	(0.61)	(0.51)
BREACH_TYPE_Stolen				-0.0017	-0.0017	-0.0017	-0.0016
				(0.40)	(0.40)	(0.39)	(0.43)
BREACH_TYPE_Lost				**0.0070****	**0.0075****	**0.0066***	**0.0066***
				(0.02)	**(0.01)**	(0.08)	(0.08)
ITG					**-0.0011**	**-0.0014**	**-0.0013**
					(0.49)	(0.43)	(0.47)
ITG_Lost						0.0021	0.0011
						(0.67)	(0.84)
Similarity							0.00101
							(0.64)
Cons	-0.0048*	-0.0092**	-0.0062	-0.0046	-0.0047	-0.0048	-0.0051
	(0.08)	(0.03)	(0.18)	(0.33)	(0.40)	(0.40)	(0.30)
N	542	468	468	468	474	474	465
adj. R-sq	0.013	0.028	0.032	0.042	0.042	0.040	0.034

p-values in parentheses: * p<.10 ** p<.05 *** p<.01 **** p<.001

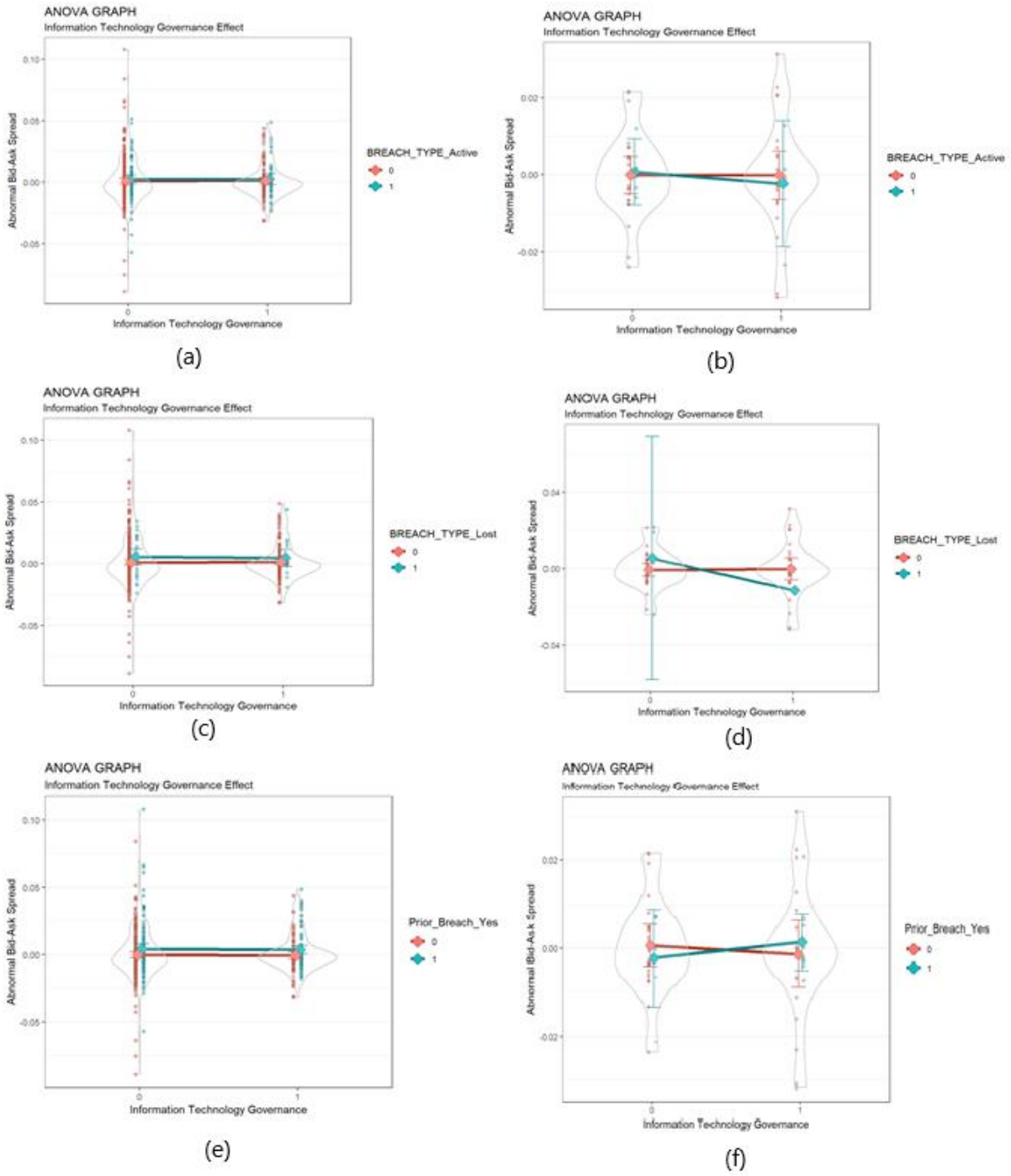


Figure 2.3 *Two-way ANOVA Unmatched Sample (a, c, e) and Matched Sample (b, d, f)*

Table 2.19

Regression Analysis for ABAS (Matched Sample)

	(1)	(2)
	ABAS (-1,0)	**ABAS (-1,0)**
ln_PRC	0.0079**	0.0058*
	(0.02)	(0.05)
Var	-0.0020	-0.0021
	(0.44)	(0.41)
Turnover	0.00037	0.00053
	(0.53)	(0.35)
In_mktCap	0.00041	0.0013
	(0.68)	(0.17)
BMRatio	-0.011	-0.012
	(0.20)	(0.22)
Leverage	-0.0045	-0.0019
	(0.63)	(0.84)
FirmType	0.0045	0.0053
	(0.52)	(0.44)
ln_BrScale	-0.00049	-0.00069
	(0.29)	(0.14)
Prior_Breach_Yes	-0.0038	-0.0023
	(0.37)	(0.58)
BREACH_TYPE_Active	0.0013	0.0021
	(0.81)	(0.69)
BREACH_TYPE_Stolen	0.00017	0.00051
	(0.97)	(0.91)
BREACH_TYPE_Lost	0.013	**0.019****
	(0.17)	**(0.03)**
ITG	0.0018	0.0023
	(0.58)	(0.47)
ITG_Lost		**-0.025****
		(0.02)
Cons	-0.023*	-0.025**
	(0.05)	(0.04)
N	58	58
adj. R-sq	0.290	0.322
p-values in parentheses: * p<.10	**p<.05 *** p<.01	**** p<.001

Cumulative Abnormal Return (CAR)

Table 2.20 is the Abnormal Return (AR) during event windows (-5, 5) for both focals and rivals. Unexpectedly, I did not find that the markets of focal firms react around

the event date, though at day 1, the abnormal return is negative. These findings are inconsistent with those of Higgs et al. (2016) and Jeong, Lee, and Lim (2018). However, the markets of rivals react significantly at day – 1. Table 2.21 presents the Cumulative Abnormal Return (CAR) of focals and rivals and it also suggests that the markets of rivals react positively at several days (-1, 1). Together, these findings suggest that the data breaches of focal firms have consequences for the markets of rival firms. However, Table 2.22 and Table 2.23 suggest the characteristics of breach types (*BREACH_TYPE_Active* and *BREACH_TYPE_Lost*) have significant negative market reactions for rival firms. In contrast, Table 2.24 suggests that *BREACH_TYPE_Stolen* has a positive effect on rivals' markets. Unexpectedly, Table 2.25 suggests that CAR between firms *ITG* = 1 and *ITG* = 0 does not differ significantly. The multivariate analysis presented in Table 2.26 further confirms that the characteristics of breach types of focals (*BREACH_TYPE_Active* and *BREACH_TYPE_Lost*) have implication for rivals. Further, it is suggested that the extent of the breach scale (*ln_BrScale*) also affects the market of rivals negatively ($\beta = -0.00087, p<0.06$). Though insignificant, the history of focals' data breaches (*Prior_Breach_Yes*) also has implications for rivals. It was not expected, but information technology governance (*ITG*) has a negative insignificant relationship with CAR. As in *ATURN* and *ABAS*, I do not find strategic similarity (*Similarity*) significant in explaining CAR.

Table 2.20

Abnormal Return (AR) of Focals and Rivals During Event Windows

Focals			Rivals		
Day	**AR**	**p-Value**	**Day**	**AR**	**p-Value**
-5	0.0021	0.16	-5	-0.0007	0.49
-4	-0.0007	0.55	-4	0.0010	0.21
-3	0.0005	0.74	-3	-0.0021	0.00 ***
-2	-0.0001	0.93	-2	0.00022	0.82
-1	0.0013	0.29	-1	0.00238	0.02 **
0	0.0009	0.48	0	-0.0008	0.41
1	-0.0011	0.48	1	0.00123	0.37
2	0.0002	0.86	2	0.00034	0.82
3	-0.0013	0.51	3	-0.0006	0.45
4	-0.0016	0.21	4	-0.0001	0.91
5	0.0012	0.43	5	-0.0004	0.68

This table reports the daily Abnormal Return (AR), along with the p-values associated with the t-tests on their significance (H0: AR = 0). *, **, *** significance at 10, 5 and 1% levels respectively.

Table 2.21

Cumulative Abnormal Return (CAR) of Focals and Rivals

Focals				Rivals			
Event Window	**CAR**	***t*-value**	***p*-value**	**Event Window**	**CAR**	***t*-value**	***p*-value**
(-1,0)	0.0021	1.23	0.89	(-1,0)	0.00154	1.06	0.14
(-1,1)	0.0011	0.49	0.69	(-1,1)	0.00278	1.41	0.08 *

This table reports the Cumulative Abnormal Return (CAR) along with the t-values and associated p values, with the Ha: CAR < 0, for Focal firms and Ha: CAR > 0, for Rival Firms. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.22

Cumulative Abnormal Return (CAR) of Rivals by BREACH_TYPE_Active

Event Window (-1,1) – Rivals			
BREACH_TYPE_Active	**CAR**	***t*-value**	***p*-value**
0	0.0059	3.39	0.00 ***
1	-0.0061		

This table reports the Cumulative Abnormal Return (CAR) along with the t-values and associated p values for the variable BREACH_TYPE_Active, with the Ha: Diff (CAR) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.23

Cumulative Abnormal Return (CAR) of Rivals by BREACH_TYPE_Lost

Event Window (-1,1) – Rivals			
BREACH_TYPE_Lost	**CAR**	***t*-value**	***p*-value**
0	0.0042	3.04	0.00 ***
1	-0.0134		

This table reports the Cumulative Abnormal Return (CAR) along with the t-values and associated p values for the variable BREACH_TYPE_Lost, with the Ha: Diff (CAR) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.24

Cumulative Abnormal Return (CAR) of Rivals by BREACH_TYPE_Stolen

Event Window (-1,1) – Rivals			
BREACH_TYPE_Stolen	**CAR**	***t*-value**	***p*-value**
0	0.0007	-2.16	0.03 **
1	0.0099		

This table reports the Cumulative Abnormal Return (CAR) along with the t-values and associated p values for the variable BREACH_TYPE_Stolen, with the Ha: Diff (CAR) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.25

Cumulative Abnormal Return (CAR) of Rivals by ITG

Event Window (-1,1) – Rivals			
ITG	**CAR**	***t*-value**	***p*-value**
0	0.0046	1.43	0.15
1	-0.0007		

This table reports the Cumulative Abnormal Return (CAR) along with the t-values and associated p values for the variable ITG, with the Ha: Diff (CAR) != 0. *, **, *** significance at 10, 5, and 1% levels, significantly.

Table 2.26

Regression Analysis for CAR (Unmatched Sample)

	Cumulative Abnormal Return					
	CAR (-1, 0)			**CAR (0, 1)**		
	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
FirmType	0.0022	0.0029	0.0029	0.0014	0.0018	0.0023
	(0.51)	(0.40)	(0.40)	(0.72)	(0.66)	(0.57)
ln_mktCap	-0.00023	0.000074	0.000100	-0.0013	-0.0012	-0.0011
	(0.77)	(0.93)	(0.90)	(0.17)	(0.21)	(0.22)
ln_BrScale	**0.00087***	**0.00089***	**0.00088***	0.00017	0.00016	0.00010
	(0.06)	(0.05)	(0.06)	(0.75)	(0.77)	(0.85)
BREACH_TYPE_Active	**0.0086****	**0.0085****	**0.0085****	**-0.012*****	**-0.012*****	**-0.013*****
	(0.03)	(0.03)	(0.04)	(0.01)	(0.01)	(0.00)
BREACH_TYPE_Stolen	0.0044	0.0044	0.0042	-0.0078	-0.0078	-0.0073
	(0.30)	(0.30)	(0.33)	(0.12)	(0.12)	(0.14)
BREACH_TYPE_Lost	**-0.015****	**-0.015****	**-0.015****	**0.029******	**0.029******	**0.028******
	(0.02)	(0.02)	(0.02)	(0.00)	(0.00)	(0.00)
Prior_Breach_Yes	-0.0035	-0.0028	-0.0028	-0.0053	-0.0049	-0.0044
	(0.33)	(0.44)	(0.44)	(0.21)	(0.25)	(0.29)
ITG		-0.0036	-0.0036		-0.0020	-0.0017
		(0.31)	(0.32)		(0.63)	(0.67)
Similarity			0.00095			0.0050
			(0.84)			(0.34)
Cons	0.014*	0.013*	0.013	0.019**	0.019**	0.016*
	(0.08)	(0.09)	(0.10)	(0.04)	(0.04)	(0.08)
N	475	475	472	475	475	472
adj. R-sq	0.030	0.031	0.027	0.025	0.023	0.024

p-values in parentheses: * p<.10 ** p<.05 *** p<.01 **** p<.001

Figure 2.4 confirms the findings discussed above for unmatched samples. However, for matched sample, it is clear that rival firms with ITG = 1 experience negative CAR for both *BREACH_TYPE_Active* and *BREACH_TYPE_Lost*. When focal firms experience BREACH_TYPE_Stolen and rivals firms have ITG = 1, the CAR of rivals reacts positively. Table 2.27 documents that markets of rival firms react positively only when they have ITG = 1 and focal firms experience stolen data breaches (*BREACH_TYPE_Stolen*). It further confirms that the scale of data breaches of focal firms has implications for rivals. To sum up, the findings suggest that though overall the markets of rivals react positively given the data breaches events of focal firms, the breach scale and the characteristics of the data breaches of focals have damaging market reaction for rival firms. Moreover, in some cases, strong corporate governance (*ITG = 1*) plays some shielding role to mitigate damages arising from the data breaches of focals.

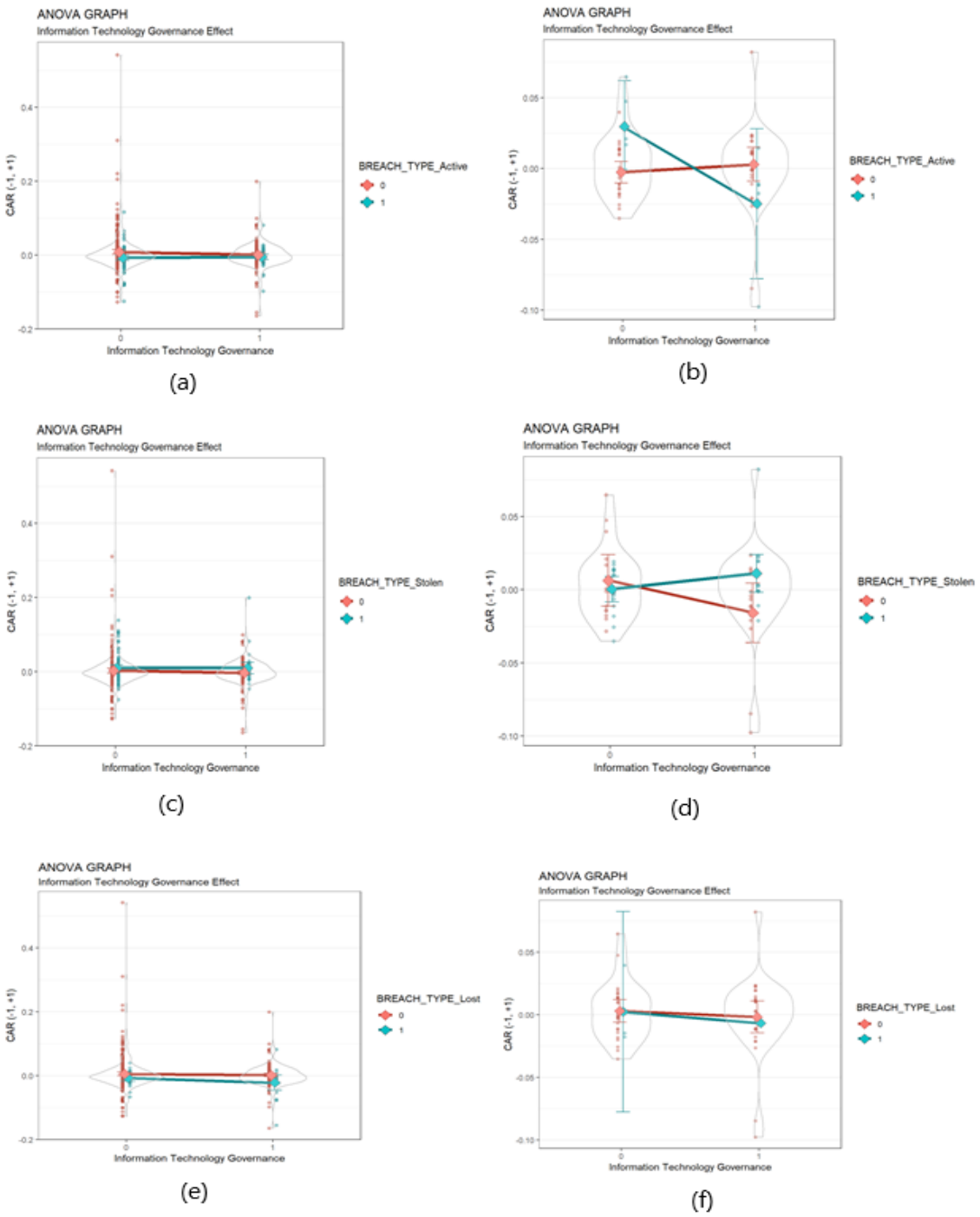


Figure 2.4 *Two-way ANOVA - Unmatched Sample (a, c, e) and Matched Sample (b, d, f)*

Table 2.27

Regression Analysis for CAR (Matched Sample)

	(1)	(2)	(3)	(4)
	CAR (-1, 1)	**CAR (-1, 1)**	**CAR (-1, 1)**	**CAR (-1, 1)**
FirmType	0.014	0.014	0.022	0.014
	(0.50)	(0.50)	(0.27)	(0.50)
ln_mktCap	0.0015	0.0015	0.0020	0.0017
	(0.46)	(0.45)	(0.31)	(0.41)
ln_BrScale	**-0.0020***	-0.0019	-0.0014	**-0.0021***
	(0.09)	(0.10)	(0.23)	**(0.09)**
BREACH_TYPE_Active	0.016	0.016	0.012	0.016
	(0.22)	(0.22)	(0.35)	(0.22)
BREACH_TYPE_Stolen	0.017*	0.017*	-0.0019	0.017*
	(0.08)	(0.09)	(0.88)	(0.08)
BREACH_TYPE_Lost	0.017	0.017	0.0088	0.023
	(0.31)	(0.33)	(0.61)	(0.26)
Prior_Breach_Yes	-0.0015	-0.0013	-0.0053	-0.0014
	(0.87)	(0.88)	(0.55)	(0.88)
ITG		-0.0017	**-0.021***	-0.00054
		(0.82)	**(0.07)**	(0.95)
ITG_Stolen			**0.034****	
			(0.03)	
ITG_Lost				-0.020
				(0.55)
Cons	-0.0077	-0.0077	-0.0038	-0.0093
	(0.75)	(0.75)	(0.87)	(0.71)
N	58	58	58	58
adj. R-sq	0.022	0.003	0.080	-0.010

p-values in parentheses *p<.10 **p<.05 ***p<.01 ****p<.001

Additional Analysis (Robustness Test)

Exclusion of Rivals That Were Also Focals

Some of the rival firms in the study are also focal firms – they experienced data breaches, as well. To ensure that the results of the study are not unduly affected by these circumstances, I exclude them and re-run the analysis. The untabulated results suggest

that the conclusions remain the same. Thus, the results of the study are not affected by inclusion in the analysis of rival firms that were also breached focal groups, as well.

Alternative Specification of Dependent Variables

To measure abnormal trading volume, many accounting researchers use median adjusted trading volume (Chen and Sami 2013, 2008). Median adjusted abnormal trading volume is the percentage of outstanding shares traded daily in the event period, less the median percentage of outstanding shares traded daily during the non-event period. Median adjusted trading volume is a better measure than mean adjusted trading volume because mean adjusted trading volume is not stable and is more easily affected by sharp increases in non-event period trading for reasons other than liquidity (Bamber 1987). When I re-run the analysis using median adjusted trading volume; the results (untabulated) are similar.

For a robustness check, I measure bid-ask spread as the absolute difference between closing bid and closing ask prices, deflated by the mid-point of the bid and ask prices. This is in line with Chen et al. (2015). The results (untabulated) also remain similar.

For CAR, I also re-run the model using a market-adjusted model. This is in line with Jeong, Lee, and Lim (2018). The market-adjusted model is very similar to the market model, except that it assumes the beta = 1. The market model might represent market risks imperfectly. The untabulated results support the original conclusion.

Discussion and Conclusion

Data breaches have become commonplace and very costly. Not only do the breached firms bear the costs of breaches, related firms are also likely to be affected by the breaches of focal firms. This research studies the reaction of the markets of rivals firms to data breaches of focal firms. The research studies trading volume, bid-ask spread, and abnormal returns of rival firms in response to the announcement of data breaches by focal firms.

The theory of competitive dynamics suggests that rival firms are likely to be affected by the data breaches of focal firms. This information transfer about such breaches between the firms occurs through two different yet significant mechanisms – the contagion effect (a negative reaction) or the competitive effect (causing a positive reaction). Under competitive dynamics, when information such as data breaches is revealed in markets, this revelation not only affects the companies concerned but can also negatively influence competitors in the industry, as well. This outcome is described as a contagion effect. Contagion effects are not limited to the effects of data breach but are also shown to have influence in many other situations. Another school of thought related to competitive dynamics suggests that there is a theoretical possibility that competitor firms may benefit from a rival's data breach. This school of thought is called the competitive effect. Prior literature related to other types of negative news releases about organizations also found support for this effect. The competitive effect holds that when a firm is in distress, rivals in the industry configure their resources accordingly and that this configuration is perceived by investors in a positive light. This market perception is revealed bidding for the rights to the residual cash flows among the firms in the industry.

So, when one firm experiences a data breach, it is natural to assume that investors will bid up competitors' stocks, thus resulting in gains. Furthermore, Signaling Theory specifies that the announcement of an event about one party will provide another party with information, thus helping the other party to infer outcomes from the announcements. Signaling theory is widely used in economics, finance, and accounting literature. The announcement of a data breach by focal firms relays information to rivals in this manner. Rivals might perceive that they need to take initiative to avoid such events in the future. Alternatively, they (rivals) might know the susceptibility of focal firms, and this might be perceived as a competitive benefit.

Using data from privacyrights.org, COMPUSTAT, CRSP, and BOARDEX, I find evidence that markets of rival firms react when focal firms experience data breach. However, the overall effects of the data breaches to rival firms are opposite to those of focal firms, and in many cases rival firms' markets also react negatively. Specifically, I find that the characteristics of data breach types and previous data breach histories of focal firms have implications for rivals. However, the existence of strong information technology governance among rivals plays a shielding role in mitigating those negative effects. Further, though I hypothesized that strategic similarity of focals with rivals also has implications, the study did not find such effect. However, the affirmative findings of the results of the study are robust to alternative specification of models and sample.

The study makes several contributions to the literature. First, the study confirms that in the event of data breaches, not only are focal firms affected, but rivals are also affected. Second, the study is the first to measure market reactions to such breaches using trading volume, which is better metric than return analysis. Third, the study also

demonstrates that data breaches of focal firms result in information asymmetry in the markets of rival firms. Finally, the findings provide some practical guidance for rival firms when their competitive counterpart experiences data breaches.

The study has some limitations. Privacyrights.org does not cover the entire population of data breaches. Therefore, the sample size is small, and this limits generality. Additionally, since disclosure of data breaches is not required by the Securities and Exchange Commission, there is wider latitude on the part of management to disclose or not disclose breaches.

CHAPTER 3

BIG DATA ANALYTICS CHALLENGES AND INTERNAL AUDIT FUNCTION (IAF)'S RELIANCE ON BIG DATA ANALYTICS

Introduction

"The world's most valuable resource is no longer oil, but data"
(The Economist 2017)

"… the development of data analytics skill is a must for accountants"
(Huerta and Jensen 2017, 104)

"Today, data analytics offers accountants opportunities to generate value"
(Schneider et al. 2015, 721)

Given the availability of vast amount of data, companies in numerous industries exploit such data for competitive advantage, aiming to either increase revenues or decrease costs. Data Driven Decisions (DDD) are making significant differences in productivity, on Return on Assets (ROA), Return on Equity (ROE), asset utilization, and on market value (Provost and Fawcett 2013). Firms using big data analytics in their operations can outperform their competitors by 5% in productivity and 6% in profitability (Barton and Court 2012). In 2017, 53% companies have adopted big data, as compared to only 17% in 2015 (Columbus 2017). Additionally, regulators are increasingly calling for organizations to use analytics (Protiviti 2017). This emphasizes the significance of big data analytics in organizations. Alles (2015) suggested that these market forces may be factors influencing auditors/accountants to embrace big data/data analytics.

Big data analytics is important for accounting profession because data gathering and analytics technologies have the potential to fundamentally change accounting and auditing task processes (Schneider et al. 2015). Scholars note that the emergence of big data analytics will significantly change the infer/predict/assure (e.g., insight/foresight/oversight) tasks performed by accountants and auditors. Big data and analytics have increasingly important implications for accounting and will provide the means to improve managerial accounting, financial accounting, and financial reporting practices (Warren, Moffitt, and Byrnes 2015). It is further suggested that big data offers an unprecedented potential for diverse, voluminous datasets and sophisticated analyses. Alles (2015) indicates that big data has great potential to produce better forecast estimates, going concern calculations, fraud, and other variables that are of concern to both internal and external auditors. Moreover, auditors might reduce audit costs and enhance profitability and effectiveness by means of big data or data analytics. Sixty-six percent of internal audit departments currently utilize some form of data analytics as part of the audit process (Protiviti 2017). Earley (2015) suggests that while there is significant promise for improving audit quality through the use of data analytics, significant hurdles still need to be overcome.

Research suggests that the accounting profession has been historically slow to embrace revolutionary technologies (Dai and Vasarhelyi 2016; M. G. Alles 2015). However, practitioners, particularly external auditors, are playing leading roles in adopting big data analytics (Deloitte 2016a; EY 2015; Fullerton 2016) and they have been documenting the barriers to the adoption of data analytics (EY 2014; KPMG 2015). Notwithstanding, there is little research about the internal auditors' adoption of big data and usage (H. Li et al. 2018; Tang, Norman, and Vendrzyk 2017) despite the fact that the Internal Audit Function (IAF) is

better positioned to leverage big data than are external auditors. The IAF has embraced analytics in the in audit process, but numerous challenges remain (Verver 2015; Protiviti 2017). In addition, research indicates that the use of audit analytics by IAF is below expectation (Li et al. 2018), but IAF still puts a high priority on data analytics and intends to increase its use in future (Tang, Norman, and Vendrzyk 2017). Although data analytics promises benefits for both external and internal auditors, it provides promising platforms for internal auditors, providing deep insights (infer), realistic foresight (predict), and continuous oversight (assure) (Schneider et al. 2015; Verver 2015). Verver (2015, 20) noted that "because internal audit has access to processes and data from across the organization, data analysis often enables auditors to provide insights into risk, control, and performance issues that no other function can provide."

Li et al. (2018) identified three factors that create unique opportunities for IAF to employ data analytics. First, the scope of tasks of IAF is much broader than that of external auditors; therefore, internal auditors should have more demand for the use of data analytics to accomplish their tasks efficiently and effectively. Second, IAFs can easily access internal organizational data, so they can easily employ data analytics to detect anomalies and fraud. Finally, the work of IAFs is not as regulated as that of external auditors; therefore, IAFs have more flexibility in exploring various data analytics tools. These three factors are also highlighted by Alles and Gray (2016) for future research opportunities.

The importance of emerging technologies such as big data analytics in IAF is demonstrated by the Institute of Internal Auditors code (2016) in its revision of the section entitled "Proficiency and Due Care" (Tang, Norman, and Vendrzyk 2017). Internal audit

departments with dedicated analytics functions experience the highest level of value from analytics, as do those departments with designated analytics champions (Protiviti 2017).

To that end, the purpose of the study is to explore the challenges to big data analytics adoption by accountants/auditors. Particularly, the study will empirically test the effect of these challenges (sometimes called barriers) on the adoption of data analytics by the IAF. Protiviti (2017, 5) noted that "demand for data analytics services from the internal audit group has increased substantially across all organizations in the last year, especially among those with IAF that have analytics champions and a dedicated analytics function. It is likely that as internal audit shops embrace analytics and achieve more progress in how they use data, this demand will continue to increase." Since data analytics has the potential to improve different aspects of auditors' work (specifically the processes of infer/predict/assure), I will explore the employment of data analytics by auditors in population tests, business process improvement, tests of regulatory compliance, identification of possible fraud, and risk or control monitoring.

The study of internal auditor reliance on big data analytics and challenges to data analytics adoption is important because big data analytics dominates the priority lists for internal auditors in the continual focus of such auditors on improving the use of data analytics to enhance technology-enabled auditing capabilities such as continuous auditing and continuous monitoring. Moreover, overcoming these constraints and challenges to the use of analytics requires a longer-term strategy and an implementation roadmap, carefully chosen and well-crafted pilot programs, and clear direction from CAEs and organizational leaders who can establish that data analytics represents a valuable facet of internal audit's services and long-term value (Protiviti 2017). Several studies (Anderson et al. 2012;

Malaescu and Sutton 2015) suggest that the investment in IT audit techniques and technology is one of the factors affecting the reliance of external auditors on IAF in keeping with requirements (PCAOB, 2007). Appelbaum (2016, 32) noted that "perhaps the genesis of a solution that addresses the challenges of external Big Data audit evidence could occur initially within the internal auditing profession." Additionally, practitioners suggest that the more mature analytics capabilities are, the greater value that analytics are perceived to deliver. To that end, our research answers the call for research by Alles and Gray (2016), Huerta and Jensen (2017), and Li et al. (2018) to investigate factors such as technical skills, business acumen, and cognitive skills related to data analytics.

The results of our study suggest that the most critical factor for big data analytics adoption is data-specific IT knowledge of accountants, rather than general IT competencies. Accountants' business knowledge and critical thinking skills are also significant. Additionally, when IAFs are tasked with fraud risk management or when IAFs work in an industry where regulation requires the use of data analytics, they are more likely to adopt big data analytics. Further analysis suggests that Chief Audit Executives (CAE) with CPA certifications are more likely to adopt big data analytics than CAEs without CPA certifications when the size of the organization is small, or when the size of the IAF is small, or when there is a lack of data-specific IT knowledge or business skills. Another important finding is that when two groups of IAFs have similar size and data-specific IT knowledge, IAFs with fraud detection responsibility (e.g., management challenges) are more likely to adopt big data analytics, thus highlighting the circumstances of the underutilization of the data analytics in many cases. Finally, IAFs in Anglo culture countries are more likely to

adopt big data analytics than IAFs in non-Anglo culture countries given that both types of IAFs have the same size and data-specific IT knowledge.

The study contributes to both theory and practice. From theoretical standpoint, first, the study empirically confirms that challenges to big data analytics have implications. Second, the findings highlight the most significant barriers that IAFs should overcome to improve the usage of big data analytics. Third, the study also documents why data analytics is sometimes underutilized even though organizations have the necessary skills to employ it. From a practical viewpoint, this study suggests how small organization or small audit departments can reap the benefits of big data analytics by employing CAEs. Second, our findings have implications for external auditors since the research suggests that the use of technology by IAFs affects external auditors' decisions regarding reliance on internal auditors.

Big Data, Data Analytics, and Audit Analytics[5]

Big Data

The meaning of big data varies across different disciplines and there is substantive confusion between the slightly differing characterizations of "big data," "business intelligence," and "data analytics" (Vasarhelyi, Kogan, and Tuttle 2015). Cao, Chychyla, and Stewart (2015, 423) indicate that "big data includes data sets that are too large and complex to manipulate or interrogate with standard methods or tools." Though many people consider big data in terms of quantities, it is also related to large-scale analysis of large amounts of data to generate insights and knowledge (Verver 2015). Big data is characterized by four Vs:

[5] In most cases, Big Data, Data Analytics, and Audit Analytics are used interchangeably.

Volume; Velocity; Variety; and Veracity. Volume refers to the size of the dataset, velocity to the speed of data generation, variety to the multiplicity of data sources, and veracity to the elimination of noise and obtaining truthful information from big data. Sometimes big data are characterized by six Vs: Volume, Velocity, Variety, Veracity, Variability, and Value; or, even seven Vs: Volume, Velocity, Variety, Veracity, Variability, Value, and Visualization (Sivarajah et al. 2017).

Data Analytics

Data analytics is defined by the AICPA (2015, 105) as "the art and science of discovering and analyzing patterns, identifying anomalies, and extracting other useful information in data underlying or related to the subject matter of an audit through analysis, modeling, and visualization for the purpose of planning or performing the audit." Cao et al. (2015, 423) define big data analytics as the process of inspecting, cleaning, transforming, and modeling big data to discover and communicate useful information and patterns, suggest conclusions, and to provide support for decision-making.

Audit Analytics[6]

Audit analytics involves the application of data analytics in the audit. Specifically, AICPA (2017) defines audit data analytics as "the science and art of discovering and analyzing patterns, identifying anomalies and extracting other useful information in data underlying or related to the subject matter of an audit through analysis, modeling and visualization for the purpose of planning or performing the audit." In other words, audit data analytics are techniques that can be used to perform a number of audit procedures such as risk assessment, tests of details, and substantive analytical procedure to gather audit

[6] This does not indicate the "Audit Analytics" database.

evidence. The benefits of using audit data analytics include improved understanding of an entity's operations and associated risk including the risk of fraud, increased potential for detecting material misstatements, and improved communications with those charged with governance of audited entities.

Related Literature

The focus of this study is on the likelihood of the adoption of big data analytics in accounting/auditing, given the challenges that exist as to its adoption. As discussed by Alles (2015), for big data usage by auditors, two scenarios can be used to predict future adoption: one is historical evidence of the adoption of technology by auditors/accountants and the other is the enthusiastic embrace of big data analytics by the clients of auditors. Therefore, a survey of the literature on the uses of big data analytics in different areas of accounting will highlight the areas in which IAFs can contribute. Additionally, a description of auditor technology adoption factors will contribute to the understanding of the context of big data analytics use.

Information Technology Acceptance and Use by Auditors

Historically, the accounting profession is not very advanced in the adoption of emerging technologies (Vasarhelyi, Kogan, and Tuttle 2015; M. G. Alles 2015). Janvrin, Bierstaker, and Lowe (2008) found that external auditors use a variety of audit applications and that the use of IT in auditing and the perceived importance of IT in auditing varies by firm size. Additionally, Janvrin, Bierstaker, and Lowe (2009) suggest that Computer Assisted Audit Tools (CAAT) are more frequently used by auditors when they obtain an understanding of client internal control systems and business processes, and computer test

controls. Moreover, their results indicate that Big Four audit firms are more likely to employ computer related audit procedures and IT specialists than are smaller audit firms.

A study by Braun and Davis (2003) suggests that while auditors perceive the benefits associated with CAAT, they lack confidence in their abilities to use it. Ahmi and Kent (2012) found that the use of Generalized Audit Software (GAS) was very low in the UK because of perceived limited benefits of GAS for small clients, because of high implementation costs, a significant learning curve, and lack of ease of use. Bierstaker, Janvrin, and Lowe (2014), using data from the Big 4, national, regional, and local audit firms, found that outcome expectations, organizational pressure, and technical infrastructure support influence the likelihood of adoption of CAAT by auditors. Gonzalez, Sharma, and Galletta (2012) found that the use of Continuous Auditing (CA) among internal auditors varies by size and is a function of effort and social influence.

Kim, Mannino, and Nieschwietz (2009), using the Technology Acceptance Model (TAM), suggest that the adoption of audit software by internal auditors is significantly influenced by Perceived Ease of Use (PEOU) and Perceived Usefulness (PU). Mahzan and Lymer (2014), using the Unified Theory of Acceptance and Use of Technology (UTAUT), suggested that performance expectancy and facilitating conditions influence internal auditors to use GAS; however, effects for social influence and effort expectancy were not significant. Curtis and Payne (2008), using experiments, indicated that given a longer-term budget and evaluation period and management favoring implementations, auditors are highly likely to adopt new technology. Pennington, Kelton, and DeVries (2006) suggest that the relationship between perceived ease of use and intention to use audit software such as Audit Command Language (ACL) is mediated by qualitative overload. Moreover, there is a positive

relationship between perception of difficulty in using ACL and perceived qualitative overload, which negatively affects the intention to employ ACL. The study by Debreceny, Lee, Neo, and Shuling Toh (2005) suggests that internal auditors treated GAS as a tool for special investigation rather than a tool for their regular work. On the other hand, external auditors did not use GAS since it was not suited for testing financial statement assertions.

Overall, this survey of the literature suggests that the adoption of technology by accountants/auditors is a function of many factors and the results of studies on the matter are mixed. Therefore, the topic of big data analytics adoption by IAFs warrants further investigation.

Prior Data Analytics/Big Data Research in Financial Accounting

Warren et al.(2015, 397) note that "in financial accounting, big data will improve the quality and relevance of accounting information, thereby enhancing transparency and stakeholder decision-making. In reporting, big data can assist with the creation and refinement of accounting standards, helping to ensure that the accounting profession will continue to provide useful information as the dynamic, real-time, global economy evolves." In particular, they suggest that big data could significantly impact the future of financial accounting and Generally Accepted Accounting Principles (GAAP). Big data can also help to supplement financial statement disclosures by accumulating, processing, and analyzing information about a given intangible of interest. Furthermore, big data or data analytics can help in narrowing the differences between accounting standards such US GAAP and International Financial Reporting Standards (IFRS) and facilitate different measurement processes such as Fair Value Accounting (FVA) by analyzing different kinds of unstructured data (Warren, Moffitt, and Byrnes 2015).

Crawley and Wahlen (2014) noted that data analytics allows researchers to explore a large amount of qualitative information disclosed by organizations, and examines the consequences of such disclosures. Moreover, data analytics now provides the opportunity to judge the informational content of qualitative financial information. For example, Davis, Piger, and Sedor (2012) found that the extent of optimism expressed in firms' earnings announcements is positively associated with Return on Assets (ROA) and stock reactions. By the same token, Li (2010c) suggested that the tone of forward-looking statements is positively associated with future earnings performance. In addition, Feldman, Govindaraj, Livnat, and Segal (2010) found that changes in disclosure tone is indicative of future changes in earnings. Interestingly, research shows that even information on social media such as Twitter can predict stock market responses (Bollen, Mao, and Zeng 2011).

Data analytics helps to relate textual data to earnings quality. For example, firms having more complicated and less transparent financial statement disclosures are more likely to have poor quality earnings, less persistent positive earnings and more persistent negative earnings (Li 2008). Li, Lundholm, and Minnis (2013) confirmed that firms discussing their competition frequently have ROAs that mean returns more severely than the firms discussing the competition infrequently.

With the help of textual data analytics, researchers recently documented the role that qualitative disclosures have in forming the information environment of organizations; such information environments include factors such as the number of analyst following a firm, characteristics of its investors, its trading activities, and the litigation it is involved with. Less readable 10-Ks are associated with greater number of analysts following the firm and a greater amount of effort needed to generate report about it (Lehavy, Li, and Merkley 2011).

They also find that less readable 10-Ks are associated with greater dispersion, lower accuracy, and greater uncertainty in analyst's earnings forecasts about a given firm. Firms having complex and less readable financial reports are also less likely to have smaller investors (Loughran and McDonald 2010; Miller 2010). Moreover, data analytics also informs investment analysis about the effects of "tone" on various risk factors such as cost of capital, volatility of stock returns, and analysts' earnings forecast dispersion (Kothari, Li, and Short 2009). Additionally, textual analytics of corporate disclosures confirms that firms are very cautious in delivering messages while facing greater litigation risks and that they reduce the levels of disclosures after litigation (Nelson and Pritchard 2007; Rogers and Van Buskirk 2009).

Like experimental studies, data analytics allows archival researchers in financial accounting to test the effect of behavioral biases of corporate executives on corporate financial policies (Li 2010b). Research documents that managers having self-serving attribution biases tend to be overconfident (Li 2010a), and the self-serving attribution bias of managers leads them to make less optimal investment decisions, to have higher leverage, to repurchase stocks, and to be unwilling to issue dividends.

Prior Data Analytics/Big Data Research in Management Accounting

Warren et al. (2015, 397) noted that "in managerial accounting, big data will contribute to the development and evolution of effective management control systems and budgeting processes." In particular, they elaborate on how big data or data analytics can play a role in management control systems by discovering behaviors that have correlation with specific goal outcomes. Essentially, big data analytics can locate new kinds of behaviors that might impact goal outcomes by simplifying the identification of important motivational

measurement tools linked to organizational goals. Moreover, by analyzing non-structured data, big data analytics can help discern employee morale, productivity, and customer satisfaction. Data analytics can also be used to improve "beyond budgeting practices" since traditional budgeting sometimes creates barriers to creativity and flexibility (Warren, Moffitt, and Byrnes 2015).

Richins, Stapleton, Stratopoulos, and Wong (2017) suggest that big data analytics could improve customer service quality. They suggest that most of the time organizations use structured data that are in their records to evaluate customer service quality; however, this approach does not take into account the customer perspective. Big data analytics allow organizations to evaluate this customer perspective by using unstructured data from social media or e-commerce sites, thus permitting organizations to have a holistic view of customer service quality.

Managers recognize that financial measures, alone, are insufficient to forecast future financial success or to use for performance management. Big data analytics provides opportunities to incorporate non-financial measures by incorporating unstructured data (Richins et al. 2017). Using big data analytics (particularly the analysis of unstructured data) accountants can identify the causes of underlying problems, understand ramifications, and develop plans to mitigate adverse impacts (Richins et al. 2017). Data analytics can also provide accountants with additional tools to monitor operations and product quality, discover opportunities to reduce costs, and contribute to decision-making (Dai and Vasarhelyi 2016).

However, research has also cautioned about the dark side of data analytics (Holt, Lang, and Sutton 2017; Warren, Moffitt, and Byrnes 2015). When used to monitor corporate performance, excessive monitoring or tracking could hinder employee creativity, motivation,

morale, and productivity. Employees may fear to demonstrate their originality and initiative. The existence of active monitoring also negatively impacts employee perceptions of organizational ethics and reduces their likelihood of being satisfied with a position in the organization (Holt, Lang, and Sutton 2017).

Prior Data Analytics/Big Data Research in Auditing

Big data analytics has the potential to improve the effectiveness of auditing by providing new forms of audit evidence. Data analytics can be used in both auditing planning and in audit procedures, helping auditors to identify and assess risk by analyzing large volumes of data. Even organizations that have very immature capabilities indicate that a strong level of value is derived from including analytics in the audit process (Protiviti 2017).

Big data is being seen by practitioners as an essential part of assurance services (Alles and Gray 2016), but its application in auditing is not as straightforward as it is in marketing and medical research. Appelbaum (2016) and Cao et al. (2015) identified several areas that are likely to benefit from the use of big data analytics. Some of the areas are:

a) At the engagement phase – supplementing auditors' industry and client knowledge
b) At the planning phase – supplementing auditors' risk assessment process
c) At the substantive test phase – verifying the management assertions
d) At the review phase – advanced data analytical tools as analytical procedures
e) At the continuous auditing phase – enhancing knowledge about the clients

Yoon, Hoogduin, and Zhang (2015) suggest that big data create great opportunities through providing audit evidence. They focused on the "sufficiency" and "appropriate" criteria and noted that though there are some issues about the propriety of big data due to different kinds of "noise," big data can be used as complementary audit evidence.

Additionally, they discussed how big data can be integrated with traditional audit evidence in order to add value in the process. Big data or data analytics can also help auditors to test the existence of assertions (e.g. fixed assets) using non-conventional data such as video recording (Warren, Moffitt, and Byrnes 2015). In the world of big data, potential types and sources of audit evidence have changed (Appelbaum 2016). For this reason, Krahel and Titera (2015) suggest that big data might change the focus of auditors, shifting emphasis from management to the verification of data.

Data quality and reliability or verifiability have become important issues in auditors' evaluations of audit evidence. In this way, big data can be used as part of analytical procedures, which are required at the planning and review phase, but which are optional at the substantive procedure phase. However, many issues remain unresolved about how to use big data since analytical procedures and auditing standards are not very specific about the selection of analytical audit procedures; the choice depends on the professional judgment of auditors (Appelbaum, Kogan, and Vasarhelyi 2017). For this reason, auditors need to exercise increased professional skepticism in the big data era because in many cases sources of big data lack provenance and, subsequently, veracity, and sometimes auditors (particularly internal auditors) have little or no involvement in data quality evaluation of such sources (Appelbaum 2016). Considering the prediction that analytics will spell the demise of auditing, Richins et al. (2017) suggest that auditors in the big data era are still essential because they know "the language of business." Particularly, they suggest that big data analytics cannot replace the professional judgment used by auditors, suggesting that analytics will instead complement auditors' professional judgment.

Alles and Gray (2016) identify four potential advantages of incorporating big data into audit practices: strong predictive power to set expectations for financial statement audits, great opportunities to identify potential fraudulent activities, increased probabilities of discovering red flags, and the possibility of developing more predictive models for going concern assumptions. To that end, internal audit groups with dedicated analytics functions and organizations that have attained a managed or optimized to the state of analytics maturity are far more likely to conduct continuous auditing (Protiviti 2017). Though big data creates many opportunities for improving auditing, it also suffers from different shortcomings that hinder its application in Continuous Auditing (CA). For example, Zhang, Yang, and Appelbaum (2015) suggest big data characteristics such as volume, velocity, variety, and veracity creates problems in its application in CA through different gaps such as data consistency, data integrity, data identification, data aggregation, and data confidentiality.

Rose, Rose, Sanderson, and Thibodeau (2017) found that the timing of the introduction of data analytics tools into the audit process affects the evaluation of evidence and professional judgment. Barr-Pulliam, Brown-Liburd, and Sanderson (2017) found that jurors consider auditors more negligent when they use traditional auditing technique rather than audit data analytics techniques. Additionally, they confirmed that audit data analytics tools increase the perceptions of audit quality. Schneider et al. (2015) suggest that data analytics can be used by auditors to evaluate the internal control effectiveness and policy compliance. They further suggest that by analyzing unusual data flows, unexpected large volumes of data, high frequency transactions, or duplicate vendor payments, auditors can better detect fraud.

Challenges to the Adoption of Data Analytics in Accounting/Auditing

The theoretical background of this research stems from the frameworks of Sivarajah et al. (2017) and Schneider et al. (2015). Sivarajah et al. (2017) identify the challenges of data analytics in terms of the data life cycle, which is depicted in Figure 3.1. They classified such issues as data challenges, process challenges, and management challenges. Schneider et al. (2015) developed a framework for data analytics organizing principles, which is depicted in Figure 3.2. In regard to the Schneider et al. framework, this study focuses on their organizing principle 3, which is called "contingency factors." I argue that both frameworks (Sivaraj and Schneider) identify data analytics challenges in the same way, but rather use different terms to describe them. I assume data challenges, process challenges, and management challenges in Sivarajah et al. (2017) are equivalent to technological factors, cognitive factors, and organization factors respectively in Schneider et al. (2015). Therefore, I develop hypotheses around these challenges. Research has identified other relevant challenges related to big data such as security, ethics, and the legal liability of auditors (Appelbaum 2016; Cao, Chychyla, and Stewart 2015; Holt, Lang, and Sutton 2017; Schneider et al. 2015; Zhang, Yang, and Appelbaum 2015), which I did not focus on for the sake of parsimony.

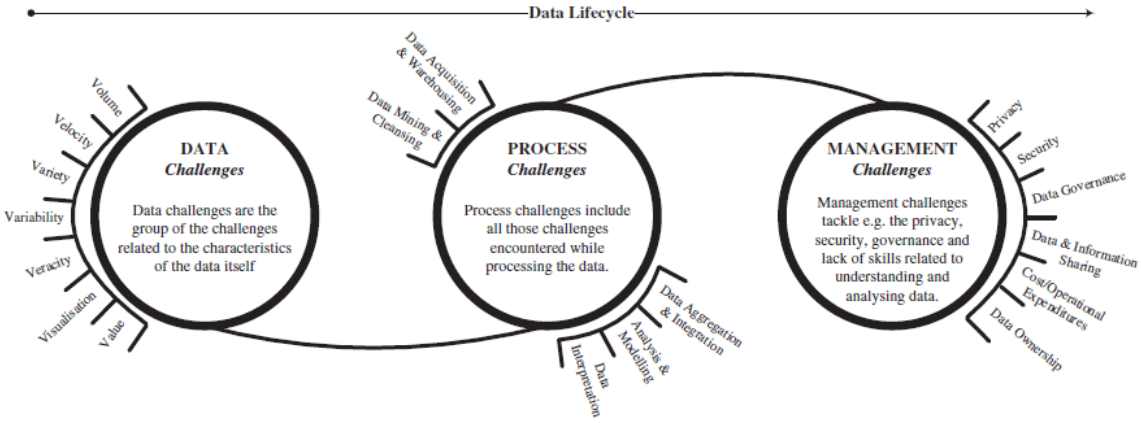


Figure 3.1 *Challenges to the Adoption of Data Analytics - Sivaraj et al. (2017)*

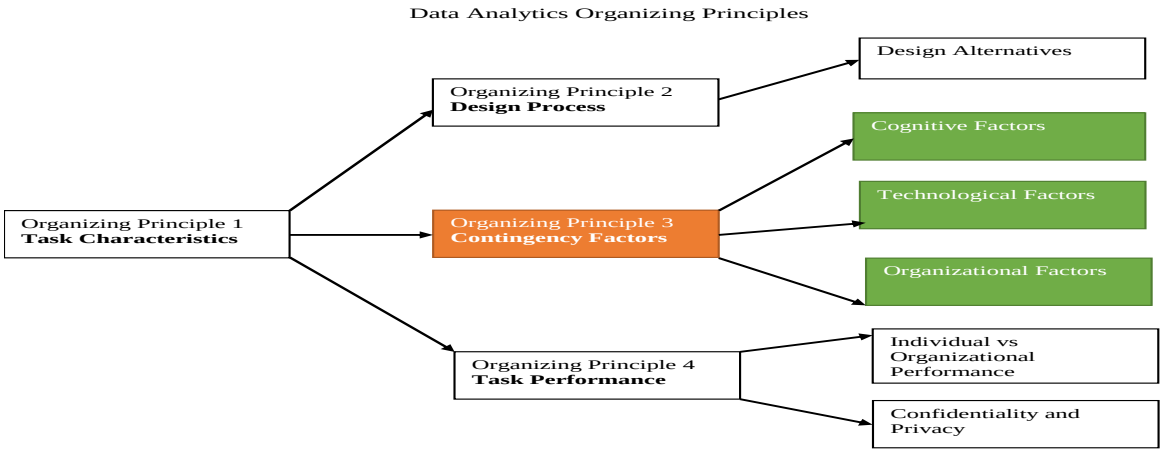


Figure 3.2 *Challenges to the Adoption of Data Analytics - Schneider et al. (2015)*

Data (Skills) Challenges

Data skills challenges involve technical competencies related to the employment of big data analytics in organization. Big data analytics capability is important for organizations because it is associated with firms' financial and market performance. Of the specific big data analytics capabilities, employee data analytics skills are one of the most important (Wamba et al. 2017).

The professional standards of internal auditors require them to have technology skills, which can largely be construed in terms of big data analytics competencies. IIA (2016, 6)

require that “Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work.” External auditors are not required to have such data analytics skills (Wang and Cuthbertson 2015). However, since PCAOB (2007) requires external auditors to rely on internal auditors, they also need to have data analytics skills to evaluate internal auditing work before relying on the IAF. These circumstances emphasize the significance of data analytics competencies in the IAF.

For the accounting practice, research has noted that most companies have developed the skills for dealing with traditional data but have not done the same for big data (Brown-Liburd, Issa, and Lombardi 2015). Implementing big data analytics is not an easy task; it requires personnel with expertise in data analytics (Cao, Chychyla, and Stewart 2015; Wang and Cuthbertson 2015). For that reason, Protiviti (2017, 6) noted that “organizations indicating that their analytics capabilities are at a higher state of maturity derive notably higher value from integrating analytics into their audit processes compared to organizations whose internal audit functions demonstrate less mature analytics capabilities. This may be because they have people with the right skillsets, unlike other internal audit organizations that are more limited in terms of analytics skills. Another possibility is that mature organizations use analytics more pervasively throughout their audit plans and processes, enabling them to glean more value from these activities.”

Emphasizing obstacles to big data adoption, Huerta and Jensen (2017, 105) commented on “…the difficulty of finding staff who can analyze businesses, identify the data needed, and determine what they tell them about the business. The creativity to ask insightful questions, paired with the analytical skills to answer them, will allow accountants to grow as

strategic business partners." Dealing with unstructured data such as text, pictures, and videos requires a new set of analytical and technical skills and technological knowledge (Huerta and Jensen 2017). PwC (2015) calls for a restructuring of accounting education, emphasizing courses related to programming, databases, multivariate and inferential statistics, and data visualization.

Alles (2015) suggested that lack of trained personnel is the greatest obstacle for the use of big data or data analytics in accounting. He also noted that auditors may find it difficult to compete for big data talent since competitors are also seeking talent for profit making rather than compliance purposes. Since big data is a disruptive technology, its adoption requires significant changes in many areas of auditing including increases in technical skills ,and the lack of these skills is one of the potential inhibitors in incorporating big data in auditing (M. Alles and Gray 2016). Deloitte (2016b) suggests that analytics might become the core capabilities for internal auditors, and it appears that CAEs are beginning to expect that all of the internal auditors in their department have a minimum level of expertise in data analytics (Tang, Norman, and Vendrzyk 2017). The average number of staff members dedicated to the data analytics function in a firm is five and the average number of data analytics function hours dedicated to audits that include analytics is 40 (Protiviti 2017).

Earley (2015) identified training and expertise of auditors as one of the three challenges affecting the use of data analytics. Regulators fear that the lack of data analytics skills among auditors might hamper the quality of auditing by focusing the shift from auditing to advisory services since the scarcity of skills might lead practitioners to hire data scientists, who have a different mindset on compliance matters than traditional auditors (Katz 2014). Li et al. (2018) also suggest that technological competence influences application-

level usage of audit analytics. Richins et al. (2017) suggests that if accountants do not extend their competencies to include data analytics skills, then they risk being replaced by data scientists. Surveys indicate that IAFs tend to lack big data analytics general technical knowledge and audit specific data analytics skills (Protiviti 2017). Figure 3.3 indicates that IAFs feel that, for general technical knowledge, their data analytics level of competency is lower, and that they have a higher need to improve it (circle 5, which is marked yellow). Similarly, for audit process knowledge, IAFs level of competency is lower and they perceive pressing needs to improve in data analytics skills and knowledge (circle one and 7, which is marked yellow, with one indicating data analytics and seven indicating data analytics tools-sampling)

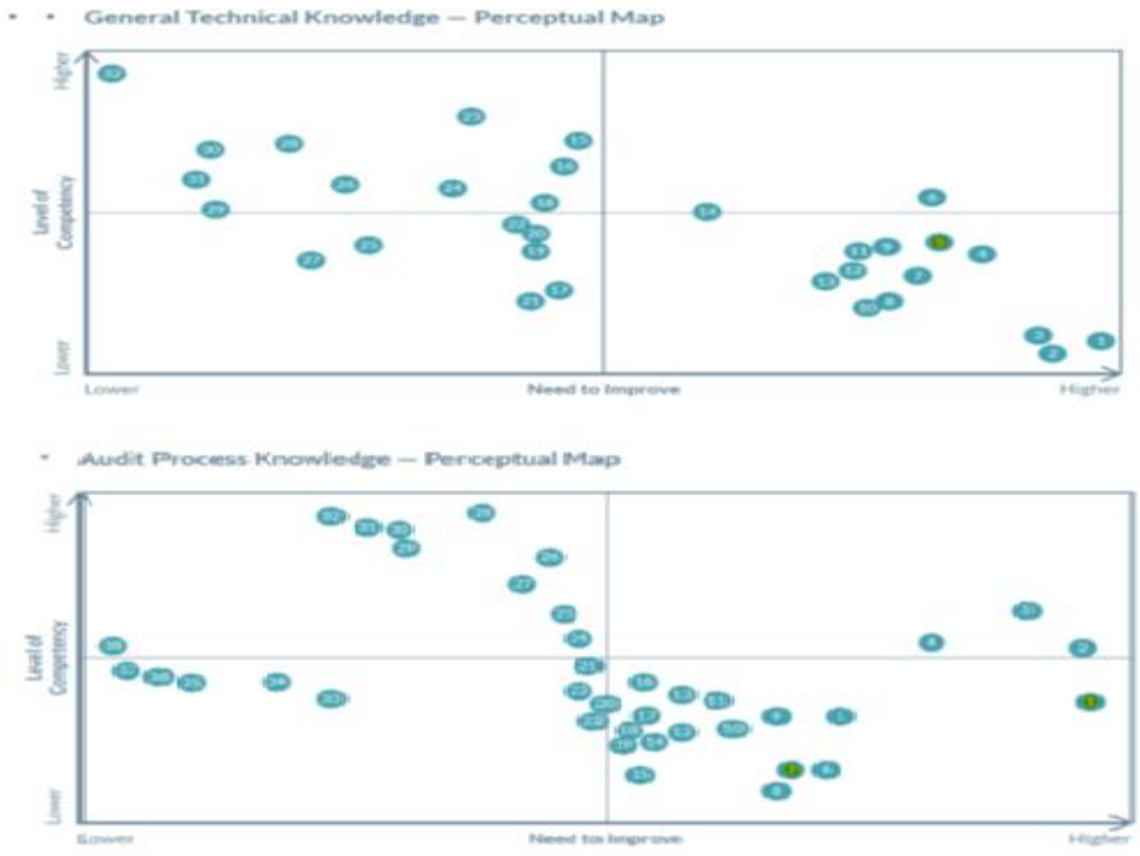


Figure 3.3 *Internal Audit Competencies - Protiviti (2017)*

From a survey of internal audit practitioners, Protiviti (2017) recommends that CAEs use champions to lead the analytics efforts because champions in analytics help bridge the gap between the analytics function and operations auditing. Additionally, the presence of champions also encourages more analytics use, including basic usage by the whole team. As compared to other organizations, those with analytics champions and dedicated analytics functions in place deliver more value, experience higher demand for their analytics services and obtain better access to higher-quality data (Protiviti 2017).

Zhang et al. (2015, 470) noted that "auditors with competence in data analytics will have better opportunities to widen the range and increase the scale of auditing on a more frequent basis via Continuous Data Monitoring (CDM), Continuous Control Monitoring (CCM), and Continuous Risk Monitoring and Assessment (CRMA)." Of the many challenges identified by Brown-Liburd et al. (2015), the lack of adequate analytics training and the absence of required analytics skills is a decisive challenge. They suggest that adequate training and skills play a critical role in adopting analytical tools. Big data creates challenges for auditors because of the associated information overload, rigors of pattern recognition, related ambiguity, and relevance, but these challenges can be overcome through data competence skills and IT savviness (Brown-Liburd et al. 2015). Additionally, Rose et al. (2017) noted that auditors' deficiencies in pattern recognition can be overcome by enhancing their knowledge. Tang et al. (2017) reported that in IAFs, a good percentage of employees hold IT related certifications. Their research implies that the demand for data analytics skills in the IAF will continue unabated and that the IAF will need more employees with data analytics skills and abilities. Therefore, I hypothesize the following:

H1a: *CAEs with IT certifications are more likely to employ data analytics in inference /prediction/assurance.*

H1b: *IT savvy IAFs are more likely to employ data analytics in inference /prediction/assurance.*

Alles (2015) suggested that since there is a lack of skilled personnel in the market and since there is severe competition for among businesses for data savvy people, training could be a better alternative to facilitate the adoption of big data. Training ensures organizational privacy, as well (Cao, Chychyla, and Stewart 2015). Richins et al.(2017) emphasized the value of training for accountants on unstructured data such as text mining, and statistical software which will help auditors to achieve high levels of efficiency and create value. Tang et al. (2017) also report that CAEs consider various data analytics tools and training to support data analytics in their respective organizations. They indicate that for improving skills in data analytics, IAFs employ different kinds of training, which can be a function of the size of the organizations and the focus of analytics. Such training is important for IAFs, because IAFs investing in training will not only be able to keep the best employees but they will also be able to attract more of the talented employees they will need in the near future (Erhardt 2016). Additionally, Braun and Davis (2003) found that additional technical training is needed and desired by auditors to increase their confidence in the use of CAATs. It seems clear that training promotes the adoption of technology by easing qualitative overload, which mediates the relationship between technology adoption intention and perceived ease of use (Pennington, Kelton, and DeVries 2006). The average number of days spent on training and development related to data analytics is nine (Protiviti 2017).

As such, I hypothesize:

H1c: *IAFs employing greater training hours in analytics are more likely to employ data analytics in inference /prediction/assurance*

Process (Cognitions) Challenges

Emphasizing the value of creative thinking in the big data era, Huerta and Jensen (2017, 102) noted that "… how the analysis of big data requires accountants to develop a creative mindset to identify the insights that can be gained from the data. Panelists emphasized that extracting meaningful knowledge from big data requires not only a deep understanding of the data, but also a creative way of thinking about data. The challenge with big data is identifying the right questions to ask." They identify four cognitive biases that might impact decision-making on whether big data analytics are used. These cognitive biases include anchoring, availability, in-attentional blindness, and confirmation bias. Anchoring involves providing responses that tend to be related to initial values. As an example of anchoring, Huerta and Jensen (2017) cited the example of the estimate of warranty expenses which are calculated using data from social media postings. Availability involves assigning greater relevance to information recently acquired than to information known earlier. In-attentional blindness involves disregarding information that is not in the specific focus of interest. Confirmation bias involves disregarding information that does not support hypothesized ideas. Lack of data interpretation skills is also identified as one of the inhibitors in incorporating big data in auditing (M. Alles and Gray 2016).

Brown-Liburd et al. (2015) suggest that although big data analytics has the potential to improve auditor judgment and decision-making, auditors need to overcome challenges related to information processing weaknesses and cognitive limitations. They identify three

ways by which big data poses challenges to auditors: extraction of large volume of nonfinancial data for which auditors are not accustomed, confusion between correlation and causation, and the unstructured nature of big data.

Though auditors lacking data analytics skill might outsource the analytics process or create tools that automate as much of the process as possible, the data analytics environment will result in auditor judgment playing a much more significant role than in sample-based auditing because of the potential for large numbers of anomalies requiring evaluation (Earley 2015). Brown-Liburd et al. (2015) and Krahel and Titera (2015) suggest that big data – a significant amount of which is unstructured and non-financial – might overwhelm the information processing capabilities of auditors. Research suggests that auditors' professional judgment is likely to be compromised by information overload (Vasarhelyi, Kogan, and Tuttle 2015). Moreover, big data will require auditors to have a higher tolerance for ambiguity and it is also likely that the use of big data will exacerbate some problems such as the tremendous number of likely exceptions – a large portion of which is likely to be false positives (Vasarhelyi, Kogan, and Tuttle 2015). However, research suggests that big data analytics provides the opportunity to reduce the number of false positives dramatically by identifying true anomalies and exceptions along with better systems of prioritization (Cao, Chychyla, and Stewart 2015).

Since skills such as pattern recognition and the related understanding of how to evaluate anomalies usually have not been the main focus of accounting education and the basis of training in public accounting firms, new auditors are not typically trained to consider whether a transaction itself makes sense or to develop expectations in order to recognize anomalies (Earley 2015). However, experience helps to compensate for the gaps (Earley

2015). Critical thinking skills deserve special attention because the possibility that the employment of big data analytics in auditing could give the mistaken impression to financial statement users that auditors are now able to provide absolute assurance rather than the customary reasonable assurance in their work (Krahel and Titera 2015). While big data analytics provides tremendous opportunities, because of information overload auditors cannot adequately capitalize on all of them; hence, they are unable to provide "absolute assurance" (Krahel and Titera 2015). Rose et al. (2017, 85) suggested that "some of the benefits of big data in audit will come from the capacity of the data to create conflict, activate skepticism, and produce judgments that combine intuition and deliberate reasoning". Therefore, I hypothesize the following:

H2: *IAFs having critical thinking skills are more likely to employ data analytics in inference /prediction/assurance.*

Management (Organizational) Challenges

Alles (2015) noted that many auditors' clients have already accepted big data; therefore, to add value for the clients and to better discharge their responsibility, auditors also face challenges in embracing big data. For internal auditors, their nature of work responsibilities will influence the extent of the usage of data analytics.

Since businesses are integrating big data with business analytics approaches to make insightful decisions, auditors have some urgency to utilize advanced data analytics tools and techniques (Appelbaum, Kogan, and Vasarhelyi 2017). To leverage the benefits of big data, both technical and business knowledge are required. In response to critics, who charge that in the accounting profession faces likely extinction in the rise of analytics, Richins et al. (2017) argues that this is not true; accountants add important value to the firm in the big data era.

They contend that to get out of the most from big data, domain-specific knowledge is also required, and accountants are highly proficient at domain-specific knowledge. In addition, accountants excel in structured data analysis. Therefore, domain-specific knowledge and skills in structured data make accountants well positioned to contribute to analyses provided by data scientists. It is further suggested that blindly following data without understanding business fundamentals can be dangerous. Rose et al. (2017) suggest that auditors who understand the client's financial issues are able to form an initial framework within which they can exercise professional skepticism and judgment, which helps to make sense of the patterns identified in big data analytics. Protiviti (2017) indicates that the most oft-cited challenge to accessing data in the organization is identifying where the data reside, and I argue that the specific business knowledge of IAFs is likely to mitigate this problem. Moreover, keen business knowledge helps identify new data sources, both internal and external, which can then enhance the internal auditor's view of risk across organizations (Protiviti 2017). As such, I hypothesize:

H3a: *Business savvy IAFs are more likely to employ data analytics in inference /prediction/assurance.*

Data analytics provides accountants with the opportunity to extend their roles – moving from watchdogs to business partners (Amato 2013). Accounting's role in strategy formulation and implementation is not new. Research suggests that historically accountants have played a significant role in strategy development and execution (Simmonds 1982). Richins et al. (2017) notes that accounting tools such as Balanced Scorecard (BSC) provide framework for examining organizations from multiple perspectives and that big data analytics can play a significant role by providing non-financial measures for performance.

Verver (2015, 20) reported that "many internal audit departments fail to make progress in implementing audit analytics because they do not treat it as a strategic initiative…" He also suggests that active involvement in data analytics increases the IAF's strategic importance in the firm and helps to deliver sustainable benefits.

Research suggests that external auditors can help their clients make better strategic decisions through the employment of data analytics tools (Earley 2015). Alles (2015) suggests that outside of auditing, big data is regarded as a tool to figure out unexpected correlations in different strategic variables which can then be exploited to increase profits (e.g. developing new marketing strategies). Moreover, he suggests that if big data truly becomes a strategic necessity for businesses, then it becomes equally necessary for auditors to be "auditing through big data." These scenarios suggest that clients have a great deal of impact on the usage of big data by auditors. These factors are called "exogenous drivers" by Alles (2015), and Richins et al. (2017) suggest that even though sometimes large datasets might find spurious correlations, accountants' abilities to understand the language of business coupled with data scientists' abilities to conduct exploratory analyses that identify correlations and patterns will turn data into implementable strategies.

However, many organizations might not employ IAFs in management positions because they may fear that it would impair the objectivity and independence of internal audit. Studies document that when IAFs act as management training ground, their objectivity (not competence) is impaired, thus affecting the financial reporting quality (Christ, Masli, et al. 2015; Rose, Rose, and Norman 2013). Therefore, even if IAFs are aligned with the strategy of an organization, their roles might be limited by different governance mechanisms such as an independent audit committee. Therefore, I hypothesize:

H3b: *IAFs that are aligned with an organization's strategy are more likely to employ data analytics in inference/ prediction (business performance).*

Data analytics in accounting is mostly used in assurance, particularly for fraud detection and compliance and in this manner data analytics helps auditors evaluate internal control effectiveness. Cao, Chychyla, and Stewart (2015) noted that the Securities and Exchange Commission (SEC) uses big data analytics to monitor market events, to figure out financial statement fraud, and to identify audit failures. They further suggest that similar analytics could also be used by auditors to identify fraudulent or high-risk activities on the part of auditees. Additionally, in many organizations the IAF uses big data analytics to identify fraudulent insurance claims (Cao, Chychyla, and Stewart 2015).

Internal auditing uses continuous monitoring of data to identify risk in internal control systems (Murphy and Tysiac 2015). Warren et al. (2015) suggest that big data will help internal auditors detect fraud more efficiently and effectively through social media text mining. Tang et al. (2017) suggest that using data analytics IAF can determine the areas for risk management in which the highest consideration should be given. Therefore, I hypothesize the following:

H3c: *IAFs with fraud detection risk responsibility are more likely to employ data analytics in assurance.*

Research Methodology

Sample

The data for the study was collected from the Common Body of Knowledge database (CBOK 2015) developed by The Institute of Internal Auditors Research Foundation (IIARF)[7]. For the study, only the responses from Chief Audit Executives (CAEs) were used since these individuals are more knowledgeable and more experienced than other staff in the internal audit department. Furthermore, the dataset represents responses from internal audit departments located in different regions of the world. The distribution of the data is given in Table 3.1 to Table 3.4.

Table 3.1

Distribution of Samples (Number of Observation)

Total Respondent	14,518
Less: Director or Senior Manager	1,630
Less: Manager	2,098
Less: Staff	5,644
Less: Missing Value for Respondents' Position	182
Less: Academic Staff or Retired	1,620
Chief Audit Executives (CAEs)	3,344
Less: Missing Values for Dependent & Independent Variables	2,356
Total Observations Used	**988**

[7] This is a proprietary database. The Appendix contains the "Agreement" between me and the IIARF, which authorizes me to use the data.

Table 3.2

Distribution of Sample (Type of Organizations)

Type_Org	Freq.	Percent
Privately Held	340	34.4%
Publicly Traded	363	36.7%
Public Sector	209	21.1%
Not for Profit	53	5.3%
Other	23	2.3%
Total	988	100%

Table 3.3

Distribution of Sample (Region Represented)

Region_Org	Freq.	Percent
Africa	101	10.2%
Asia	191	19.3%
Europe	279	28.2%
Latin America	119	12.0%
North America	273	27.6%
Oceania	25	2.5%
Total	988	100%

Table 3.4

Distribution of Sample (Country Represented)

Country	Freq.	Percent
Not an IIA Member	19	1.9%
Albania	2	0.2%
Argentina	14	1.4%
Armenia	3	0.3%
Australia	22	2.2%
Austria	7	0.7%
Bahamas	1	0.1%
Bangladesh	1	0.1%
Barbados	2	0.2%

Table 3.4 (Continued)

Belgium	6	0.6%
Bolivia	2	0.2%
Bosnia & Herzegovina	1	0.1%
Botswana	1	0.1%
Brazil	12	1.2%
Bulgaria	1	0.1%
Canada	34	3.4%
Cayman Islands	1	0.1%
Chile	25	2.5%
China	11	1.1%
Taiwan	13	1.3%
Colombia	13	1.3%
Costa Rica	6	0.6%
Croatia	1	0.1%
Cyprus	2	0.2%
Czech Republic	1	0.1%
Denmark	10	1.0%
Dominican Republic	4	0.4%
Ecuador	8	0.8%
Egypt	1	0.1%
El Salvador	8	0.8%
Estonia	8	0.8%
Ethiopia	2	0.2%
Fiji	2	0.2%
Finland	2	0.2%
Macedonia	3	0.3%
France	39	3.9%
Germany	13	1.3%
Greece	7	0.7%
Haiti	2	0.2%
Honduras	2	0.2%
Hong Kong	1	0.1%
Hungary	1	0.1%
Iceland	1	0.1%

Table 3.4 (Continued)

India	26	2.6%
Indonesia	12	1.2%
Israel	12	1.2%
Italy	16	1.6%
Japan	7	0.7%
Kenya	2	0.2%
South Korea	2	0.2%
Latvia	3	0.3%
Lebanon	3	0.3%
Lithuania	3	0.3%
Luxembourg	2	0.2%
Malawi	1	0.1%
Malaysia	33	3.3%
Mauritius	7	0.7%
Mexico	8	0.8%
Montenegro	1	0.1%
Netherlands	7	0.7%
New Zealand	5	0.5%
Nicaragua	4	0.4%
Nigeria	2	0.2%
Norway	4	0.4%
North America	9	0.9%
Oman	5	0.5%
Panama	5	0.5%
Paraguay	1	0.1%
Peru	8	0.8%
Philippines	8	0.8%
Poland	2	0.2%
Puerto Rico	1	0.1%
Qatar	3	0.3%
Romania	1	0.1%
Russia	5	0.5%
Saudi Arabia	9	0.9%
Serbia	5	0.5%

Table 3.4 (Continued)

Singapore	7	0.7%
Slovenia	5	0.5%
South Africa	36	3.6%
Spain	27	2.7%
Sri lanka	3	0.3%
Swaziland	1	0.1%
Sweden	6	0.6%
Switzerland	45	4.5%
Tanzania	19	1.9%
Thailand	1	0.1%
Tunisia	2	0.2%
Turkey	11	1.1%
Uganda	10	1.0%
United Arab Emirates	21	2.1%
United Kingdom & Ireland	13	1.3%
United States	217	22.0%
Uruguay	5	0.5%
Zimbabwe	14	1.4%
Member at large - Not Affiliated	5	0.5%
Total	985	100%

Variables Measurement

Research indicates that IAFs employ data analytics in different kinds of functions such as audit execution, audit planning, fraud investigation, continuous monitoring, risk assessment, continuous auditing, reporting, testing of entire population, trend analysis, sample selection, testing of individual controls, audit scoping and so forth (Protiviti 2017) . However, this study focuses on the five areas in which IAFs are most likely to employ big data analytics: testing of entire populations rather than sampling, tests for regulatory compliance, identification of possible instances of fraud, issues discovered through risk or

control monitoring, and business improvement opportunities. Protiviti (2017) noted that 77% of organizations use big data analytics in the testing of entire populations and 66% use it for sample selection; 11% use big data analytics for departmental governance and 47% use it for continuous monitoring. In addition, 54% of IAFs use data analytics in fraud investigation and 46% use it for risk assessment. Therefore, this study covers a well-represented sample of areas in which IAFs employ big data analytics. Since the dependent variable used here is a categorical variable, logistic regression is employed for analysis. Table 3.5 represents the metrics for variables in the study.

Table 3.5

Measurement of Variables

Variables	**CBOK (2015) Questions**	**Definition**
Dependent Variables		
DA_IP_Pop (Infer/Predict/Assure)	Q96	1 if IAF uses data mining or data analytics for tests of entire populations rather than sampling; zero otherwise.
DA_IP_BusImp (Infer/Predict)	Q96	1 if IAF uses data mining or data analytics for business improvement opportunities; zero otherwise.
DA_Assu_Reg (Assure)	Q96	1 if IAF uses data mining or data analytics for tests of regulatory compliance; zero otherwise.
DA_Assu_Fraud (Assure)	Q96	1 if IAF uses data mining or data analytics for the identification of possible frauds; zero otherwise.
DA_Assu_RCMoni (Assure)	Q96	1 if IAF uses data mining or data analytics for risk or control monitoring; zero otherwise.
Independent Variables		
cert_IT	Q13	1 if CAE has IS certification such as CISA, QiCA, CRISC; zero otherwise

Table 3.5 (continued)

IT_Savvy_GEN[8]	Q95 (95-1, 95-2, 95-7,95-8,95-9,95-10,95-11	Factor scores were calculated, using Bartlett method.
IT_Savvy_Data	Q95 (95-3, 95-4, 95-5, 95-6)	Factor scores were calculated, using Bartlett method.
LogTraining_hours	Q14	Natural log of the number of hours of formal training related to the internal audit profession
Critical_Thinking	Q86	Factor scores were calculated, using Bartlett method.
Business_Savvy	Q82	Factor scores were calculated, using Bartlett method.
Strategic_alignment	Q57	1 if IAF is fully aligned with the strategic plan of organization; zero otherwise.
Fraud_DetRes	Q55	1 if IAF has all or most of the responsibility to detect fraud in the organization; zero otherwise.
Control Variables		
Size_Org	Q19	Natural log of the number of Full Time Employees (FTE) in organizations
LogAC_Meetings	Q78a	Log of the number of Audit Committee or equivalent Meetings held last year.

For H1a, CAEs' certifications in information technology are measured using a dummy variable, with one representing CAEs having Information Systems (IS) certifications. For H1b, factor analysis was conducted since the variable is a latent construct. Table 3.6 contains the items indicating the constructs. When factor analysis was performed, two eigenvalues greater than one were found; therefore, two latent constructs were formed, with one being labelled general-IT savviness (*IT_Savvy_GEN*) and the other data-specific IT savviness (*IT_Savvy_Data*). General IT savviness (*IT_Savvy_GEN*) refers to the typical IT

[8] When I run exploratory factor analysis on Q95, I got two factors with Eigenvalue greater than 1. Therefore, I created two constructs; *IT_Savvy_GEN* for the first factor and *IT_Savvy_Data* for the second factor. The items for each construct are in the parentheses of the second column.

competencies of IAFs whereas specific IT savviness (*IT_Savvy_Data*) refers to the data-oriented competencies of IAFs. The items of the constructs are self-explanatory. The factor loadings of both constructs (*IT_Savvy_GEN* & *IT_Savvy_Data*) are documented in Table 3.6, with each loading being above the recommended threshold as suggested by Hair et al. (1998).

Table 3.6

Items to Measure Latent Construct

Constructs	**Measures**
Business_Savvy	Estimate your proficiency for each competency using the following scale; 1-Novice = can perform routine tasks with direct supervision; 2-Trained = can perform routine tasks with limited supervision; 3-Competent = can perform routine tasks independently; 4- Advanced = can perform advanced tasks independently; 5- Expert = can perform complex advanced tasks independently. 1. Understanding the organization's internal control risks (BS1) 2. Understanding the organization's strategic risks (BS2) 3. Understanding the organization's governance risks (BS3) 4. Understanding the organization's industry and economic factors affecting it (BS4) 5. Understanding the organization's business objectives (BS5)
IT_Savvy_GEN	What is the extent of activity for your internal audit department related to the use of the following IT tools and techniques? 1 = None; 2 = Minimal; 3= Moderate; 4= Extensive 1. A Software or a tool for internal audit risk assessment (ITSG1) 2. An automated tool for internal audit planning and scheduling (ITSG2) 3. Electronic Workpapers (ITSG3) 4. Flowchart or Process Mapping Software (ITSG4) 5. Internal Quality Assessments using an automated tool (ITSG5) 6. An automated tool to monitor and track audit remediation and follow up (ITSG6) 7. An automated to manage the information collected by internal audit (ITSG7)

Table 3.6 (Continued)

IT_Savvy_Data	What is the extent of activity for your internal audit department related to the use of the following IT tools and techniques? 1 = None; 2 = Minimal; 3= Moderate; 4= Extensive 1. A software or tool for data mining (ITSD1) 2. An automated tool for data analytics (ITSD2) 3. Computer Assisted Audit Technique (ITSD3) 4. Continuous/Real time Auditing (ITSD4)
Critical_Thinking	Estimate your proficiency for each competency using the following scale; 1-Novice = can perform routine tasks with direct supervision; 2-Trained = can perform routine tasks with limited supervision; 3-Competent = can perform routine tasks independently; 4- Advanced = can perform advanced tasks independently; 5- Expert = can perform complex advanced tasks independently. 1.Use appropriate data collection tools to create audit efficiency (CT1) 2.Use data analysis to reach meaningful conclusions (CT2) 3.Apply problem solving techniques to address issues (CT3) 4. Apply understanding of the organization's business objectives and strategy (CT4)

To calculate the factor scores, the Bartlett method was used. For H1c, training (*LogTraining_hours*) was measured using the log of the number of training hours IAFs usually receive in a given year. The critical thinking skills (*Critical_Thinking*) of IAFs were measured using factor analysis and the Bartlett method was used. Table 3.6 includes the items for this latent construct and Table 3.7 includes factor loadings of the items. All of the loadings of the construct of critical thinking skills (*Critical_Thinking*) are above the recommended threshold as suggested by Hair et al. (1998), but the measure CT4 is cross loaded with other construct; therefore, measure CT4 is excluded while calculating factor scores since it violates discriminant validity of the construct. For H3a, business savviness of IAFs (*Business_Savvy*) is measured using the items listed in Table 3.6 and the factor loadings are listed in Table 3.7. As was the case with the previous constructs, this construct's factor loadings are also above the recommended threshold. As stated, item CT4 is not counted towards business savviness in order to avoid violations of discriminant validity. For H3b,

strategic alignment of IAFs (*Strategic_alignment*) is measured using a dummy variable, with one being the IAFs fully aligned with strategic plan of the organization or zero otherwise. Similarly, for H3c, fraud detection responsibility (*Fraud_DetRes*) is measured by using a dummy variable and one represents the IAFs responsible for all or most of the fraud in the organizations or zero otherwise.

Table 3.7

Factor Loadings (Principal Component Factor with Varimax Rotation)

Items	Business_Savvy	IT_Savvy_GEN	IT_Savvy_Data	Critical_Thinking
ITSG1	0.1385	**0.6350**	0.3914	0.0343
ITSG2	0.1153	**0.6754**	0.4544	0.0056
ITSG3	0.143	**0.7174**	-0.0044	0.0267
ITSG4	-0.0041	**0.5988**	0.1377	0.1955
ITSG5	-0.0061	**0.6783**	0.386	0.111
ITSG6	0.1363	**0.7128**	0.3135	-0.0425
ITSG7	0.0731	**0.7589**	0.359	0.0312
ITSD1	0.1465	0.1937	**0.8149**	0.0574
ITSD2	0.0899	0.2456	**0.8335**	0.0858
ITSD3	0.0056	0.2974	**0.7660**	0.0834
ITSD4	-0.0539	0.3797	**0.6322**	0.2194
BS1	**0.8391**	0.0183	0.0564	0.1628
BS2	**0.8665**	0.0657	0.053	0.224
BS3	**0.8504**	0.0458	0.0814	0.2142
BS4	**0.8205**	0.1202	0.0793	0.1777
BS5	**0.8516**	0.0909	0.0372	0.223
CT1	0.3025	0.0376	0.1149	**0.8511**
CT2	0.3396	0.0115	0.1197	**0.8554**
CT3	0.4892	0.0828	0.031	**0.6886**
CT4	**0.6744**	0.0684	-0.0141	**0.5311**

Control Variables

The literature suggests a range of potential control variables that influence information technology adoption, and these have been included in the models. They are discussed below.

Size_Org: The use of IT in auditing and the perceived importance of IT is largely a function of organization size (Janvrin, Bierstaker, and Lowe 2008). Tang et al. (2017) also indicate that firm size affects the decision to provide training related to different kinds of efficiencies to auditors. Large organizations are well positioned to adopt disrupting technologies such as big data analytics because they have better resources for acquisition and implementation. Therefore, it is expected that large organizations are more likely to employ big data analytics in different aspects of operation, including the internal audit function. The variable that assesses this capability is called *Size_Org* and is measured using the log of the number of a firm's full-time employees. Using full-time employee for measurement is ideal for the purposes of this study because it avoids exchange rate problems - the data for this study originating in different geographical locations of the world.

LogAC_Meetings/LogAC_IAF_Meetings: Internal auditors play a critical role in the governance of organizations; they play a key role in helping audit committees discharge their responsibilities. Since big data analytics provides greater opportunities in organizational governance through risk control monitoring, fraud identification, and regulatory compliance, it is very likely that audit committees might be favorably inclined toward the adoption of analytics technology to optimize the effectiveness of the audit committee's oversight. Research confirms that audit committees are influential in the implementation of various emerging technologies and processes such as Extensible Business Reporting Language (XBRL) and cybersecurity audit (Abdolmohammadi et al. 2017; Islam, Farah, and Stafford 2018). Corporate governance guidelines emphasize frequent audit committee meetings in order to facilitate better communication between audit committees and internal auditors (PCAOB 2012; Blue Ribbon Committee 1999); it is also the case that auditor meetings with

their audit committees reduce the probability of fraud and restatement of financial statements (Abbott, Parker, and Peters 2004; Beasley, Carcello, and Hermanson 1999).

Therefore, it is argued that because of the beneficial possibilities arising from implementation of big data analytics in corporate governance, audit committees might lead IAFs to choose to employ big data analytics. Two variables were used to measure this role of board oversight: *LogAC_Meetings* represents the log of the number of audit committee meetings (or equivalent) and *LogAC_IAF_Meetings* represents the log of the number of audit committee meetings in which the Chief Audit Executive (CAEs) is invited to attend.

*Industry_Org:*Of the companies adopting big data, telecommunication and financial service are in the lead (Columbus 2017). Many financial services organizations have a requirement that all audits use data analytics, or that the auditors validate that they reviewed their scope and approach for data analytics use and can justify why analytics cannot be used (Protiviti 2017). Therefore, the dummy variable *Industry_Org* is included, with one referring to the organizations belonging to financial or insurance industry or zero otherwise.

Cert_CPA/Cert_CIA: Tang et al. (2017) confirm that CPA and CIA certification are the most common credentials held by members of the IAF. Even so, internal audit professionals who desire to elevate their data analytics capabilities are uncertain about how to accomplish this task (Protiviti 2017), and it is well established that certification represents the specialization related to knowledge. Therefore, two variables are included to represent the specialization of CAEs - *Cert_CPA* (1 for the CAEs with CPA certification or zero otherwise) and *Cert_CIA* (1 representing the CAEs with CIA certification).

*LogExp_CAE:*As discussed by Earley (2015), experience might compensate for the gap between education and training in big data, so CAE experience might serve as an analog

to education or certifications in regard to the use of big data analytics in internal auditing. Given the issues related to the use of big data such as information overload and ambiguity, Brown-Liburd et al. (2015) suggest that less experienced auditors face problems in exercising professional judgment in its use. They call for future research on the influence of experience in its effect on big data usage. Rose et al. (2017) also found that auditing experience has an effect on the understanding of data patterns in big data analytics. However, CAE experience might also have an inconclusive effect on big data adoption because research does indicate that CAEs with more experience in place might prefer either traditional alternative or emerging technologies (Abdolmohammadi and Boss 2010). The variable representing the CAE experience is called *LogExp_CAE*, which is the log of the number of years of experience as CAE.

LogAge_IAF: Research indicates that the average number of years that a dedicated analytics function might be in place is four years (Protiviti 2017). This suggests that mature IAFs are more likely to be involved with emerging areas such as XBRL implementation or security auditing (Héroux and Fortin 2013; Abdolmohammadi et al. 2017; Islam, Farah, and Stafford 2018). For that reason, it is expected that the more mature IAFs are, the greater the likelihood of adopting big data analytics. The variable used to measure the maturity of the IAF is *LogAge_IAF*, which is the log of the number of years that IAFs have been in the organization.

*LogSize_IAF:*Research indicates that IAF size might also have a considerable effect on its ability to contribute to big data analytics adoption (Tang, Norman, and Vendrzyk 2017). The literature indicates that Big four audit firms are more likely to employ computer-related audit procedures and IT specialists than are smaller audit firms (Janvrin, Bierstaker,

and Lowe 2009). Larger internal audit functions with more advanced analytics capabilities utilize data analytics in a majority of the audits they perform; larger internal audits can build repeatable or self-service tools that businesses can use without internal audit being closely involved (Protiviti 2017). Since size of internal audit seems to be a determining factor, the variable called *LogSize_IAF* is specified to investigate the effect, and it is characterized by the log of the number of Full Time Employees (FTE) in the IAF.

Budget: The research by Protiviti (2017) and Tang et al. (2017) indicates that many IAFs consider their budget to be a barrier to the adoption of big data analytics. Long term budgets can influence the adoption process for audit software by auditors (Curtis and Payne 2008). It appears that less than 67% of internal audit functions are associated with 20% of the total budget dedicated to data analytics (Protiviti 2017). For that reason, the variable *Budget* is specified using a dummy variable, with one representing completely sufficient budget or zero otherwise.

ACCountries: Cultural change represents a major obstacle to successful implementation of analytics (Protiviti 2017). Practitioners suggest that scarcity of skills related to data analytics is more acute in developing economies than it is in developed economies. The oversight of boards might not be as rigorous in developing countries as in the developed ones, as well - thus potentially overlooking the potential of big data analytics in risk control monitoring, risk assessment, fraud detection, and regulatory compliance in lesser developed nation contexts. Therefore, it is expected that the adoption of big data analytics might differ in different national settings. The variable *ACCountries* is a categorical variable, with one representing respondents belonging to Anglo-culture countries such as UK/Ireland; USA; Canada; Australia; New Zealand; or South Africa, zero otherwise.

Empirical Models

In this study, the use of big data analytics was tested in five areas: data mining/data analytics for tests of entire populations rather than sampling, analytics for business improvement opportunities, analytics for tests of regulatory compliance, analytics for the identification of fraud, and analytics for risk or control monitoring. For this reason, five separate logistic regression models were used. The models are given below; some of the explanatory variables of the models differ because of the change of the nature of the relationship with dependent variables.

$$Prob\ (DA\_IP\_Pop = 1) = F\ [\alpha_0 + \alpha_1\ Size\_Org + \alpha_2\ LogAC\_Meetings + \alpha_3\ LogAC\_IAF\_Meetings + \alpha_4\ Industry\_Org + \alpha_5\ cert\_CPA + \alpha_6\ cert\_CIA + \alpha_7\ LogExp\_CAE + \alpha_8\ LogAge\_IAF + \alpha_9\ LogSize\_IAF + \alpha_{10}\ Budget + \alpha_{11}\ ACCountries + \alpha_{12}\ cert\_IT + \alpha_{13}\ IT\_Savvy\_GEN + \alpha_{14}\ IT\_Savvy\_Data + \alpha_{15}\ LogTraining\_hours + \alpha_{16}\ Critical\_Thinking + \alpha_{17}\ Business\_Savvy + \alpha_{18}\ Strategic\_alignment + \alpha_{19}\ Fraud\_DetRes] + \boldsymbol{\varepsilon} \quad \text{Eq. (3.1)}$$

$$Prob\ (DA\_IP\_BusImp = 1) = F\ [\beta_0 + \beta_1\ Size\_Org + \beta_2\ LogAC\_Meetings + \beta_3\ LogAC\_IAF\_Meetings + \beta_4\ Industry\_Org + \beta_5\ cert\_CPA + \beta_6\ cert\_CIA + \beta_7\ LogExp\_CAE + \beta_8\ LogAge\_IAF + \beta_9\ LogSize\_IAF + \beta_{10}\ Budget + \beta_{11}\ ACCountries + \beta_{12}\ cert\_IT + \beta_{13}\ IT\_Savvy\_GEN + \beta_{14}\ IT\_Savvy\_Data + \beta_{15}\ LogTraining\_hours + \beta_{16}\ Critical\_Thinking + \beta_{17}\ Business\_Savvy + \beta_{18}\ Strategic\_alignment] + \boldsymbol{\varepsilon} \quad \text{Eq. (3.2)}$$

$$Prob\ (DA\_Assu\_Reg = 1) = F\ [\gamma_0 + \gamma_1\ Size\_Org + \gamma_2\ LogAC\_Meetings + \gamma_3\ LogAC\_IAF\_Meetings + \gamma_4\ Industry\_Org + \gamma_5\ cert\_CPA + \gamma_6\ cert\_CIA + \gamma_7\ LogExp\_CAE + \gamma_8\ LogAge\_IAF + \gamma_9\ LogSize\_IAF + \gamma_{10}\ Budget + \gamma_{11}\ ACCountries + \gamma_{12}\ cert\_IT + \gamma_{13}\ IT\_Savvy\_GEN + \gamma_{14}\ IT\_Savvy\_Data + \gamma_{15}\ LogTraining\_hours + \gamma_{16}\ Critical\_Thinking + \gamma_{17}\ Business\_Savvy + \gamma_{18}\ Fraud\_DetRes] + \boldsymbol{\varepsilon} \quad \text{Eq. (3.3)}$$

$$Prob\ (DA\_Assu\_Fraud= 1) = F\ [\delta_0 + \delta_1\ Size\_Org + \delta_2\ LogAC\_Meetings + \delta_3\ LogAC\_IAF\_Meetings + \delta_4\ Industry\_Org + \delta_5\ cert\_CPA + \delta_6\ cert\_CIA + \delta_7\ LogExp\_CAE + \delta_8\ LogAge\_IAF + \delta_9\ LogSize\_IAF + \delta_{10}\ Budget + \delta_{11}\ ACCountries + \delta_{12}\ cert\_IT + \delta_{13}\ IT\_Savvy\_GEN + \delta_{14}\ IT\_Savvy\_Data + \delta_{15}\ LogTraining\_hours + \delta_{16}\ Critical\_Thinking + \delta_{17}\ Business\_Savvy + \delta_{18}\ Fraud\_DetRes] + \boldsymbol{\varepsilon} \quad \text{Eq. (3.4)}$$

$$Prob\ (DA\_Assu\_RCMoni = 1) = F\ [\varphi_0 + \varphi_1\ Size\_Org + \varphi_2\ LogAC\_Meetings + \varphi_3\ LogAC\_IAF\_Meetings + \varphi_4\ Industry\_Org + \varphi_5\ cert\_CPA + \varphi_6\ cert\_CIA + \varphi_7\ LogExp\_CAE + \varphi_8\ LogAge\_IAF + \varphi_9\ LogSize\_IAF + \varphi_{10}\ Budget + \varphi_{11}\ ACCountries + \varphi_{12}\ cert\_IT + \varphi_{13}\ IT\_Savvy\_GEN + \varphi_{14}\ IT\_Savvy\_Data + \varphi_{15}\ LogTraining\_hours + \varphi_{16}\ Critical\_Thinking + \varphi_{17}\ Business\_Savvy + \varphi_{18}\ Fraud\_DetRes] + \boldsymbol{\varepsilon} \quad \text{Eq. (3.5)}$$

Results

Descriptive Analysis of Variables

Summary statistics in Table 3.8 shows that 59% of IAFs use big data analytics to test entire populations rather than sampling (*DA_IP_Pop*) and this use is statistically significant across type of organization ($\chi^2 = 14.36$; $p < 0.01$). 56% of IAFs use data analytics for fraud detection (*DA_Assu_Fraud*), with $\chi^2 = 6.23$ and $p < 0.18$, indicating that there is no difference across different types of organizations in the use of data analytics in this manner. 39% of IAFs use big data analytics for tests of regulatory compliance (*DA_Assu_Reg*), with statistically significant differences across organization type ($\chi^2 = 15.14$; $p < 0.00$). Of all five of the modelled uses of data analytics, analytics for business improvement opportunities (*DA_IP_BusImp*) scores lowest (31%), with differences across organization not significant ($\chi^2 = 3.46$; $p < 0.48$). This implies that the application of data analytics in business improvement process by IAFs is limited. This finding makes sense as the increased corporate governance practice around the world tries to mitigate the use of IAFs as management operation ground.

Table 3.8

Summary Statistics Across Types of Organizations [mean (standard deviation]

Variables	Full Dataset	Privately Held	Publicly Traded	Public Sector	Not for Profit	Other	F-Statistics/ $\chi 2$ (Sig)
DA_IP_Pop	0.59	0.60	0.64	0.49	0.49	0.61	14.36
	(0.49)	(0.49)	(0.48)	(0.50)	(0.51)	(0.50)	(0.01)
DA_IP_BusImp	0.31	0.33	0.31	0.28	0.28	0.43	3.46
	(0.46)	(0.47)	(0.46)	(0.45)	(0.46)	(0.51)	(0.48)
DA_Assu_Reg	0.39	0.46	0.35	0.33	0.49	0.48	15.14
	(0.49)	(0.50)	(0.48)	(0.47)	(0.51)	(0.51)	(0.00)
DA_Assu_Fraud	0.56	0.55	0.60	0.49	0.55	0.61	6.23
	(0.50)	(0.50)	(0.49)	(0.50)	(0.50)	(0.50)	(0.18)
DA_Assu_RCMoni	0.46	0.44	0.47	0.44	0.45	0.52	1.42
	(0.50)	(0.50)	(0.50)	(0.50)	(0.50)	(0.51)	(0.84)
cert_IT	0.16	0.13	0.17	0.15	0.25	0.30	9.75
	(0.36)	(0.33)	(0.37)	(0.36)	(0.43)	(0.47)	(0.05)
IT_Savvy_GEN	0.00	0.14	0.02	-0.19	-0.27	-0.02	4.58
	(1.00)	(1.00)	(1.00)	(0.99)	(1.02)	(0.99)	(0.00)
IT_Savvy_Data	0.00	0.10	0.03	-0.19	-0.20	0.18	3.69
	(1.00)	(1.00)	(1.00)	(1.01)	(0.98)	(0.90)	(0.01)
LogTraining_hours	3.70	3.71	3.65	3.79	3.78	3.64	2.20
	(0.59)	(0.67)	(0.57)	(0.48)	(0.40)	(0.63)	(0.07)
Critical_Thinking	0.00	(0.03)	0.01	-0.01	0.20	-0.10	0.64
	(1.00)	(0.99)	(1.02)	(1.02)	(0.95)	(0.89)	(0.63)
Business_Savvy	0.00	-0.06	0.03	-0.05	0.30	0.09	1.69
	(1.00)	(1.03)	(0.99)	(1.01)	(0.84)	(0.76)	(0.15)
Strategic_alignment	0.63	0.64	0.59	0.67	0.64	0.70	5.33
	(0.48)	(0.48)	(0.49)	(0.47)	(0.48)	(0.47)	(0.26)
Fraud_DetRes	0.20	0.17	0.22	0.16	0.28	0.26	6.82
	(0.40)	(0.38)	(0.41)	(0.37)	(0.46)	(0.45)	(0.15)
Size_Org	7.05	6.53	7.67	7.01	6.55	6.37	12.22
	(2.35)	(2.21)	(2.48)	(2.09)	(2.35)	(2.63)	(0.00)
LogAC_Meetings	1.72	1.69	1.78	1.68	1.65	1.71	2.17
	(0.51)	(0.55)	(0.48)	(0.49)	(0.45)	(0.65)	(0.07)
LogAC_IAF_Meetings	1.64	1.63	1.67	1.62	1.61	1.66	0.48
	(0.50)	(0.53)	(0.49)	(0.47)	(0.50)	(0.67)	(0.75)
Industry_Org	0.35	0.54	0.29	0.15	0.38	0.39	92.87
	(0.48)	(0.50)	(0.45)	(0.36)	(0.49)	(0.50)	(0.00)
cert_CPA	0.44	0.42	0.44	0.44	0.45	0.57	1.91
	(0.50)	(0.50)	(0.50)	(0.50)	(0.50)	(0.51)	(0.75)
cert_CIA	0.41	0.39	0.39	0.45	0.58	0.30	10.15
	(0.49)	(0.49)	(0.49)	(0.50)	(0.50)	(0.47)	(0.04)
LogExp_CAE	1.90	1.91	1.87	1.89	1.94	2.03	0.39
	(0.72)	(0.73)	(0.69)	(0.74)	(0.73)	(0.78)	(0.82)
LogAge_IAF	2.60	2.50	2.69	2.62	2.60	2.71	2.64
	(0.80)	(0.79)	(0.78)	(0.84)	(0.78)	(0.83)	(0.03)
LogSize_IAF	2.14	2.04	2.31	2.09	1.77	2.21	3.84
	(1.22)	(1.21)	(1.19)	(1.23)	(1.26)	(1.30)	(0.00)
Budget	0.35	0.35	0.37	0.30	0.34	0.48	5.08
	(0.48)	(0.48)	(0.48)	(0.46)	(0.48)	(0.51)	(0.28)
ACCountries	0.32	0.22	0.32	0.40	0.74	0.17	64.30
	(0.47)	(0.42)	(0.47)	(0.49)	(0.45)	(0.39)	(0.00)
N	988.00	340.00	363.00	209.00	53.00	23.00	

Finally, it is clear that of all the types of organizations (except the "other" category), analytics find greater uses in tests of entire populations, for fraud detection, and in risk control monitoring for publicly traded organizations. For independent variables, it is found that only 16% of IAFs have CAEs with information technology/systems certifications (*cert_IT*), with the differences across type of organization statistically significant ($\chi^2 = 9.75$; $p < 0.05$). For general IT savviness (*IT_Savvy_GEN*) the mean value is zero with standard deviation 1. Since the Bartlett method standardizes the factor scores, it always produces a mean of zero and a standard deviation of 1. However, the mean value for general IT savviness is positive for privately held and publicly traded organization, suggesting that privately held and publicly traded organizations' general IT savviness is greater than that of other types of organizations in the analysis (significant at $F = 4.58$; $p < 0.00$). The same is true for data-specific IT savviness (*IT_Savvy_Data*), with significant differences across organization type ($F = 3.69$; $p < 0.01$). For training hours, the mean of the log of training is 3.70 and is statistically significant ($F = 2.20$; $p < 0.07$). For critical thinking (*Critical_Thinking)*, the overall mean is zero (standard deviation 1), with the mean of publicly traded organizations and not-for-profit organizations being positive, indicating that they have greater critical thinking skills than other types of organizations; however, the differences for critical thinking skills (*Critical_Thinking)* are not statistically significant ($F = 0.64$; $p < 0.63$). The differences in the mean of business savviness of IAFs (*Business_Savvy*) across organization type are not statistically significant ($F = 1.69$; $p < 0.15$). Furthermore, 63% of IAFs are found to be fully aligned with the strategic plan of the organization (*Strategic_alignment*), with the IAFs in publicly traded organizations having the lowest relation with strategic alignment. The differences of strategic alignment of IAFs across

organization type are not statistically significant ($\chi^2 = 5.33$ $p < 0.26$). Twenty percent of IAFs are responsible for fraud detection in their organization (Fraud_*DetRes*), but differences across organizational type are not statistically significant ($\chi^2 = 6.82$; $p < 0.15$).

For control variables, it is found that the average size of organizations (*Size_Org*) is 7.05, which is significant across organizational type ($F = 12.22$; $p < 0.00$), and publicly traded companies are the largest in size (average size – 7.67). Furthermore, the number of audit committee meetings (*LogAC_Meetings*) is significantly different across organization type ($F = 2.17$; $p < 0.07$), with an average meeting number of 1.72. Even so, the average number of audit committee meetings in which CAEs are invited (*LogAC_IAF_Meetings*) are not statistically significant across organization type ($F = 0.48$; $p < 0.75$). Thirty-five percent of organizations in the sample belong to the financial or insurance industry, and it was found that the average percentage of CAEs having CPA certifications (*cert_CPA*) was 44%, even though that was not statistically significant across organization type ($\chi^2 = 1.91$; $p < 0.75$). On the other hand, differences in CIA certification across different types of organizations (*cert_CIA*) are statistically significant ($\chi^2 = 10.15$; $p < 0.04$), with an average certification rate for percentage of CAEs of 41%. This finding related to CPA and CIA certification in organizations is consistent with prior research (Tang, Norman, and Vendrzyk 2017).

No differences were found for experience of CAEs (*LogExp_CAE*) across types of organizations ($F = 0.39$; $p < 0.82$), but there is significant difference in the maturity of IAFs (*LogAge_IAF*) across organization type ($F = 2.64$; $p < 0.03$). Similarly, the size of IAFs (*LogSize_IAF*) across types of organizations is significant ($F = 3.84$; $p < 0.00$). Also, 35% of IAFs appear generally to have sufficient budgets (*Budget*), with the differences across different types of organizations not statistically significant ($\chi^2 = 5.08$; $p < 0.28$). Finally, 32%

of our sample is from Anglo-culture countries. These descriptive analyses suggest that there are sufficient variations in the various explanatory variables related to data analytics to accurately account for the usage of data analytics by the internal audit function.

Univariate Tests of Hypotheses

Table 3.9 tests the relationship of explanatory variables with the dependent variables specified for the study. The analysis from the variable of IT certification of CAEs (*cert_IT*) suggests that IT certification has a role in the use of big data analytics in tests of populations rather than samples ($\chi^2 = 6.329$; $p < 0.012$), but *cert_IT* is not significant in any other area of analytics usage of data analytics. Hence, there is marginal support for hypothesis H1a. Regarding H1b, IT competencies, both general and data-specific, are significant across all dependent variables, confirming that IT competencies of IAFs are highly likely to lead to the adoption of analytics in accounting and auditing practice. The same is true for IAFs providing greater training to their employees, which supports H1c.

H2 tests for the effect of critical thinking skills in the IAF and subsequent adoption of analytics technology. Not surprisingly, when assessing the role of the presence of critical thinking in the IAF and subsequent intentions to use analytics for specific purposes related to business goals, differences are significant and in the expected direction for all dependent variables. It appears that the presence of critical thinking skills in the IAF has an important effect on the uses of big data analytics for solving key auditing and business problems.

H3a speculates on the business savviness of IAFs and its relationship to the adoption and use of big data analytics and is significant across all dependent variables. IAF's that have a good understanding of business processes are more likely to employ analytics in their practices. H3b probes the strategic alignment of the IAF with the adoption of data analytics.

Table 3.9

Summary Statistics Across Dependent Variables

		DA_IP_Pop					**DA_IP_BusImp**					**DA_Assu_Reg**					**DA_Assu_Fraud**					**DA_Assu_RCMoni**				
		Yes		No		Stat (p value)	Yes		No		Stat (p value)	Yes		No		Stat (p value)	Yes		No		Stat (p value)	Yes		No		Stat (p value)
		579	59%	409	41%		308	31%	680	69%		389	39%	599	61%		551	56%	437	44%		450	46%	538	54%	
cert_IT	Yes	105	18%	50	12%	$\chi2$ = 6.329 (0.012)	53	17%	102	15%	$\chi2$ = 0.781 (0.377)	59	15%	96	16%	$\chi2$ = 0.132 (0.717)	91	17%	64	15%	$\chi2$ = 0.644 (0.422)	71	16%	84	16%	$\chi2$ = 0.005 (0.944)
	No	474	82%	359	88%		255	83%	578	85%		330	85%	503	84%		460	83%	373	85%		379	84%	454	84%	
IT_Savvy_GEN	Mean		0.19		-0.27	t = -7.29 (0.000)		0.2		-0.09	t = -4.34 (0.000)		0.23		-0.15	t = -5.93 (0.000)		0.19		-0.24	t = -6.92 (0.000)		0.24		-0.2	t = -7.04 (0.000)
	SD		0.04		0.04			0.06		0.04			0.05		0.04			0.04		0.05			0.05		0.04	
IT_Savvy_Data	Mean		0.36		-0.51	t = -14.77 (0.000)		0.3		-0.14	t = -6.46 (0.000)		0.32		-0.21	t = -8.32 (0.000)		0.34		-0.43	t = -12.94 (0.000)		0.3		-0.25	t = -8.88 (0.000)
	SD		0.036		0.05			0.06		0.04			0.05		0.04			0.04		0.04			0.05		0.04	
LogTraining_hours	Mean		3.75		3.65	t = -2.44 (0.007)		3.72		3.7	t = -0.62 (0.268)		3.76		3.66	t = -2.64 (0.004)		3.73		3.67	t = -1.60 (0.055)		3.74		3.67	t = -1.75 (0.041)
	SD		0.02		0.03			0.04		0.02			0.03		0.02			0.02		0.03			0.03		0.02	
Critical_Thinking	Mean		0.07		-0.09	t = -2.44 (.0074)		0.17		-0.08	t = -3.53 (.0000)		0.2		-0.13	t = -5.05 (0.000)		0.1		-0.12	t = -3.43 (0.000)		0.11		-0.09	t = -3.15 (0.000)
	SD		0.04		0.05			0.06		0.04			0.05		0.04			0.04		0.05			0.05		0.04	
Business_Savvy	Mean		0.12		-0.17	t = -4.47 (0.000)		0.12		-0.05	t = -2.46 (0.007)		0.14		-0.09	t = -3.47 (0.000)		0.09		-0.11	t = -3.16 (0.000)		0.12		-0.1	t = -3.41 (0.000)
	SD		0.04		0.05			0.06		0.04			0.05		0.04			0.04		0.05			0.05		0.04	
Strategic_alignment	Yes	380	66%	242	59%	$\chi2$ = 4.29 (0.038)	213	69%	409	60%	$\chi2$ = 7.38 (0.007)	270	69%	352	59%	$\chi2$ = 11.46 (0.001)	358	65%	264	60%	$\chi2$ =2.17 (0.140)	302	67%	320	59%	$\chi2$ =6.12 (0.013)
	No	199	34%	167	41%		95	31%	271	40%		119	31%	247	41%		193	35%	173	40%		148	33%	218	41%	
Fraud_DetRes	Yes	109	19%	84	21%	$\chi2$ = .447 (0.504)	65	21%	128	19%	$\chi2$ = .701 (0.402)	91	23%	102	17%	$\chi2$ = 6.08 (0.014)	123	22%	70	16%	$\chi2$ =6.16 (0.013)	104	23%	89	17%	$\chi2$ =6.73 (0.010)
	No	470	81%	325	79%		243	79%	552	81%		298	77%	497	83%		428	78%	367	84%		346	77%	449	83%	
Size_Org	Mean		7.33		6.65	t = -4.48 (0.000)		7.2		6.98	t = -1.37 (0.086)		6.83		7.19	t = 2.39 (0.990)		7.31		6.71	t = -3.99 (0.000)		7.22		6.9	t = -2.14 (0.016)
	SD		0.1		0.11			0.13		0.09			0.12		0.09			0.1		0.11			0.11		0.1	
LogAC_Meetings	Mean		1.72		1.71	t = -0.49 (0.313)		1.72		1.71	t = -0.31 (0.378)		1.77		1.68	t = -2.79 (0.003)		1.73		1.71	t = -0.63 (0.264)		1.72		1.71	t = -0.15 (0.441)
	SD		0.02		0.02			0.03		0.02			0.03		0.02			0.02		0.02			0.02		0.02	
LogAC_IAF_Meetings	Mean		1.67		1.6	t = -1.942 (0.026)		1.64		1.64	t = -0.13 (0.449)		1.71		1.6	t = -3.19 (0.000)		1.66		1.62	t = -1.37 (0.086)		1.65		1.63	t = -0.49 (0.313)
	SD		0.02		0.02			0.03		0.02			0.03		0.02			0.02		0.02			0.02		0.02	
Industry_Org	Yes	205	35%	143	35%	$\chi2$ = .021 (0.886)	95	31%	253	37%	$\chi2$ = 3.76 (0.052)	177	46%	171	29%	$\chi2$ = 29.71 (0.000)	183	33%	165	38%	$\chi2$ =2.21 (0.137)	167	37%	181	34%	$\chi2$ =1.29 (0.256)
	No	374	65%	266	65%		213	69%	427	63%		212	55%	428	72%		368	68%	272	62%		283	63%	357	66%	
cert_CPA	Yes	288	50%	147	36%	$\chi2$ = 18.53 (0.000)	140	46%	295	43%	$\chi2$ = 0.37 (0.54)	175	45%	260	43%	$\chi2$ =0.24 (0.625)	247	45%	188	43%	$\chi2$ =0.32 (0.570)	195	43%	240	45%	$\chi2$ =0.16 (0.687)
	No	291	50%	262	64%		168	55%	385	57%		214	55%	339	57%		304	55%	249	57%		255	57%	298	55%	
cert_CIA	Yes	249	43%	158	39%	$\chi2$ = 1.89 (0.169)	129	42%	278	41%	$\chi2$ =0.09 (0.767)	149	38%	258	43%	$\chi2$ =2.21 (0.137)	237	43%	170	39%	$\chi2$ =1.70 (0.192)	176	39%	231	43%	$\chi2$ =1.48 (0.224)
	No	330	57%	251	61%		179	58%	402	59%		240	62%	341	57%		314	57%	267	61%		274	61%	307	57%	

Table 3.9 (Continued)

LogExp_CAE	Mean		1.94		1.84	t = -2.16 (0.016)		1.84		1.92	t = 1.69 (0.954)		1.95		1.86	t = -1.72 (0.043)		1.91		1.88	t = -0.64 (0.262)		1.89		1.91	t = 0.45 (0.673)
	SD		0.03		0.03			0.04		0.03			0.04		0.03			0.03		0.03			0.03		0.03	
LogAge_IAF	Mean		2.69		2.48	t = -4.06 (0.000)		2.55		2.63	t = 1.52 (0.935)		2.68		2.55	t = -2.54 (0.006)		2.65		2.55	t = -2.05 (0.020)		2.67		2.55	t = -2.50 (0.006)
	SD		0.03		0.04			0.04		0.03			0.04		0.03			0.03		0.04			0.04		0.03	
LogSize_IAF	Mean		2.32		1.88	t = -5.73 (0.000)		2.14		2.14	t = 0.07 (0.528)		2.32		2.03	t = -3.67 (0.000)		2.29		1.95	t = -4.33 (0.000)		2.34		1.97	t = -4.89 (0.000)
	SD		0.05		0.06			0.07		0.05			0.07		0.05			0.05		0.06			0.06		0.05	
Budget	Yes	224	39%	120	29%	$\chi2$ = 9.23 (0.002)	123	40%	221	33%	$\chi2$ = 5.16 (0.023)	148	38%	196	33%	$\chi2$ =2.95 (0.086)	207	38%	137	31%	$\chi2$ =4.15 (0.042)	167	37%	177	33%	$\chi2$ =1.92 (0.166)
	No	355	61%	289	71%		185	60%	459	68%		241	62%	403	67%		344	62%	300	69%		283	63%	361	67%	
ACCountries	Yes	209	36%	110	27%	$\chi2$ = 9.28 (0.002)	99	32%	220	32%	$\chi2$ =0.00 (0.948)	109	28%	210	35%	$\chi2$ =5.34 (0.021)	183	33%	136	31%	$\chi2$ =0.49 (0.485)	153	34%	166	31%	$\chi2$ =1.11 (0.292)
	No	370	64%	299	73%		209	68%	460	68%		280	72%	389	65%		368	67%	301	69%		297	66%	372	69%	

With the exception of the identification of fraud (*DA_Assu_Fraud*, $\chi^2 = 2.17$; $p < 0.14$), it is significant to the adoption of data analytics. Moreover, when IAFs are tasked with the fraud detection, they are also significantly more likely to adopt big data analytics for fraud detection, regulatory compliance, and risk control monitoring, thus supporting H3c. Overall, the several tests of variables spanning H1 (a,b,c), H2, and H3 (a,b,c) provide strong support for the hypothesized influences of IAF competencies and skills in leading to the adoption/usage of big data analytics in different areas of accounting and audit.

For control variables, it is found that organization size (*Size_Org*) is significant across all dependent variable in explaining the usage of data analytics. The board governance variables (*LogAC_Meetings; LogAC_IAF_Meetings*) also provide marginal support for usage of big data analytics. Additionally, IAFs in financial or insurance industries are significantly likely to engage in adoption of big data analytics for business improvement processes and in assuring regulatory compliance. This finding is line with the practitioner surveys on the topic (Protiviti 2017). CAEs with CPA certification are highly likely to adopt big data analytics in testing of populations; however, CIA certification is not significant for any of the dependent variables. Additionally, CAE experience, the age of IAFs, and the size of IAFs also indicate support for the usage of big data analytics, as does the presence of an adequate IAF budget. Lastly, and in some cases, there are differences in the adoption of big data analytics between Anglo-culture and non-Anglo culture countries.

Multivariate Analysis and Tests of Hypotheses

The correlation matrix in Table 3.10 demonstrates that all correlations between explanatory variables are below 0.50, except for the correlation between *LogAC_Meetings* and *LogAC_IAF_Meetings*, which is 0.884. However, tests of Variance Inflation Factor (VIF) for these variables returns a result of less than 10, which overcomes speculation that there might be multi-collinearity problems with the model.

Table 3.11 through 3.15 document the results of the multivariate logistic regression. Since in logistic regression analysis it is difficult to interpret the beta coefficients, the marginal effects of means in addition to the beta coefficients are also calculated (marginal effects at means are in brackets). In order to measure the goodness of fit, Percentage of Correctly Predicted (PCP), which measures the percentage of the respondent correctly predicted by the respective models is calculated. In calculating PCP, the cutoff point is 0.50.

Table 3.11 (Equation 1) displays results for adoption of big data analytics for testing of populations rather than samples. The results demonstrated in the table suggest that data-specific IT competencies (*IT_Savvy_Data*) and business savviness (*Business_Savvy*) are significant in predicting the usage of big data analytics by IAFs for purposes of testing population rather than sample, and this supports hypotheses H1b and H3a. Additionally, it is found that organizational size (*Size_Org*), audit committee and IAF meetings (*LogAC_IAF_Meetings*), CPA certification (*cert_CPA*), and size of IAFs (*LogSize_IAF*) are significant in explaining the usage of big data analytics by the IAF, as well.

Table 3.10

Correlation Matrix

	Size_Org	LogAC_Meetings	LogAC_IAF_Meeting	Industry_Org	cert_CPA	cert_CIA	LogExp_CAE	LogAge_IAF	LogSize_IAF	Budget	AC Countries	cert_IT	IT_Savvy_GEN	IT_Savvy_Data	Log Training	Critical_Thinking	Business_Savvy	Strategic_alignment	Fraud_DetRes
Size_Org	1																		
LogAC_Meetings	0.0625*	1																	
LogAC_IAF_Meetings	0.0589	0.884***	1																
Industry_Org	-0.198***	0.139***	0.178***	1															
cert_CPA	-0.0053	-0.011	0.0122	0.0119	1														
cert_CIA	0.0471	-0.0438	-0.0473	-0.0833**	0.0282	1													
LogExp_CAE	0.0196	0.0362	0.0699*	0.0107	0.0903**	0.101**	1												
LogAge_IAF	0.178***	0.100**	0.122***	0.159***	0.0278	-0.0281	0.238***	1											
LogSize_IAF	0.336***	0.126***	0.123***	0.0643*	0.0587	-0.00751	0.0700*	0.364***	1										
Budget	0.0573	0.0263	0.021	0.106***	0.058	0.00557	0.0277	0.143***	0.101**	1									
ACCountries	0.0947**	-0.00292	0.0435	-0.0424	0.199***	0.165***	0.137***	0.0900**	-0.012	0.036	1								
cert_IT	0.0226	0.0226	0.0369	-0.00347	0.0603	0.244***	0.0338	-0.0285	0.0317	0.0352	0.0950**	1							
IT_Savvy_GEN	0.0979**	0.0932**	0.117***	0.135***	0.0104	-0.0605	0.0907**	0.217***	0.282***	0.176***	-0.0482	0.0061	1						
IT_Savvy_Data	0.124***	0.0869**	0.128***	0.0955**	0.0832**	-0.00093	0.132***	0.221***	0.272***	0.150***	0.0226	0.0749*	0.670***	1					
LogTraining_hours	0.0393	0.136***	0.154***	0.0624	0.113***	0.196***	0.139***	0.109***	0.0659*	0.0717*	0.0424	0.117***	0.182***	0.171***	1				
Critical_Thinking	0.0321	0.0283	0.0253	-0.00405	-0.0882**	-0.0113	0.0683*	-0.0094	0.0008	0.0583	-0.0251	0.0423	0.187***	0.228***	0.0987**	1			
Business_Savvy	0.0923**	-0.0316	-0.00746	0.0332	-0.0232	0.0334	0.127***	0.0760*	0.0452	0.127***	0.0694*	0.0467	0.213***	0.181***	0.144***	0.665***	1		
Strategic_alignment	0.0272	0.0689*	0.0942**	0.0786*	-0.0796*	-0.00097	-0.004	0.0277	0.0472	0.134***	-0.0889**	-0.0091	0.183***	0.152***	0.0921**	0.142***	0.196***	1	
Fraud_DetRes	-0.0577	-0.0162	-0.0307	-0.0213	-0.0564	-0.0493	0.0032	0.0279	0.0447	0.0043	-0.116***	-0.0441	0.0317	0.0691*	-0.0032	0.0680*	0.0003	0.0819**	1
* p<0.05	** p<0.01	*** p<0.001																	

Table 3.11

Regression Results and Marginal Effect at Means (Testing of Population)

	Hypothesis	Model (1) DA_IP_Pop	Model (2) DA_IP_Pop	Model (3) DA_IP_Pop	Model (4) DA_IP_Pop
DA_IP_Pop					
Size_Org		0.07262[0.018]**	0.06976[0.017]**	0.06959[0.017]**	0.05770[0.014]
		(0.0232)	(0.0449)	(0.0456)	(0.1012)
LogAC_Meetings		-0.7280[-0.176]**	-0.5927[-0.141]*	-0.5942[-0.141]*	-0.5170[-0.123]
		(0.0124)	(0.0633)	(0.0629)	(0.1095)
LogAC_IAF_Meetings		0.7956[0.192]***	0.5351[0.127]*	0.5370[0.128]*	0.5099[0.122]
		(0.0073)	(0.0988)	(0.0980)	(0.1205)
Industry_Org		-0.03257[-0.0079]	-0.1052[-0.025]	-0.1046[-0.025]	-0.1543[-0.036]
		(0.8284)	(0.5220)	(0.5245)	(0.3539)
cert_CPA		0.4809[0.116]***	0.4212[0.100]***	0.4246[0.101]***	0.4222[0.100]***
		(0.0006)	(0.0059)	(0.0059)	(0.0067)
cert_CIA		0.1265[0.031]	0.1024[0.024]	0.1033[0.025]	0.09130[0.022]
		(0.3662)	(0.5237)	(0.5205)	(0.5721)
LogExp_CAE		0.05773[0.014]	-0.03637[-0.009]	-0.03739[-0.009]	-0.06578[-0.016]
		(0.5588)	(0.7360)	(0.7293)	(0.5465)
LogAge_IAF		0.1137[0.028]	0.03363[0.008]	0.03456[0.008]	0.02846[0.007]
		(0.2349)	(0.7489)	(0.7425)	(0.7882)
LogSize_IAF		0.2404[0.058]***	0.1270[0.030]*	0.1279[0.030]*	0.1356[0.032]*
		(0.0006)	(0.0793)	(0.0779)	(0.0645)
Budget		0.3046[0.074]**	0.1930[0.046]	0.1923[0.046]	0.1537[0.037]
		(0.0354)	(0.2278)	(0.2296)	(0.3428)
ACCountries		0.2255[0.054]	0.2656[0.063]	0.2662[0.063]	0.2017[0.047]
		(0.1396)	(0.1122)	(0.1115)	(0.2356)
cert_IT	**H1a**		0.2205[0.052]	0.2194[0.052]	0.2156[0.051]
			(0.3116)	(0.3143)	(0.3270)
IT_Savvy_GEN	**H1b**		-0.2759[0.066]***	-0.2766[0.066]***	-0.3278[0.078]***
			(0.0085)	(0.0084)	(0.0021)
IT_Savvy_Data	**H1b**		1.1228[0.267]***	1.1204[0.266]***	1.1764[0.279]***
			(0.0000)	(0.0000)	(0.0000)
LogTraining_hours	**H1c**		-0.03725[-0.009]	-0.03908[-0.009]	-0.07303[-0.017]
			(0.7757)	(0.7657)	(0.5819)
Critical_Thinking	**H2**			0.01348[0.003]	-0.2015[-0.048]*
				(0.8578)	(0.0512)

Table 3.11 (Continued)

Business_Savvy	**H3a**				0.3281[0.079]*** (0.0019)
Strategic_alignment	**H3b**				0.03965[0.009] (0.8042)
Fraud_DetRes	**H3c**				-0.2202[-0.051] (0.2415)
_cons		-1.5384**** (0.0001)	-0.4303 (0.4599)	-0.4267 (0.4639)	-0.1702 (0.7758)
LR chi2		78.96 (0.000)	235.59 (0.000)	235.62 (0.000)	247.79 (0.000)
N		988	988	988	988
pseudo R-sq		0.0589	0.1758	0.1758	0.1842
Percentage of Correctly Predicted (Goodness-of-fit)		62.45%	72.37%	72.27%	71.05%
p-values in parentheses; Marginal Effect at Means in brackets					
* p<.10		** p<.05	*** p<.01	**** p<.001	

It is evident that the probability of adopting big data analytics in testing of populations is 10% greater for CAEs with CPA certification than the CAEs without CPA certification (marginal effects at means). The model's PCP is more than 70%, thus confirming that the model accurately classifies 70% of the data. To gain additional insights from the interaction of the significant variables, I tested the marginal change of the probability of adoption of big data analytics for testing of populations, which is explained in the additional analysis section of the paper.

Table 3.12 (Equation 2) provides results for the analysis of the adoption of big data analytics for business improvement process. It is evident that data-specific IT competencies (*IT_Savvy_Data*) and critical thinking skills (*Critical_Thinking*) are statistically significant, with a PCP of 70.04%, thus supporting hypotheses H1b and H2.

Table 3.12

Regression Results and Marginal Effect at Mean (Business Improvement Process)

	Hypotheses	(1) DA_IP_BusImp	(2) DA_IP_BusImp	(3) DA_IP_BusImp	(4) DA_IP_BusImp
DA_IP_BusImp					
Size_Org		0.03417[0.007]	0.03002[0.006]	0.02864[0.006]	0.02830[0.006]
		(0.2988)	(0.3731)	(0.3968)	(0.4056)
LogAC_Meetings		0.05666[0.012]	0.1952[0.041]	0.1777[0.037]	0.1999[0.042]
		(0.8442)	(0.5165)	(0.5580)	(0.5119)
LogAC_IAF_Meetings		0.03568[0.008]	-0.1632[-0.034]	-0.1475[-0.031]	-0.1829[-0.038]
		(0.9034)	(0.5954)	(0.6343)	(0.5567)
Industry_Org		-0.2713[-0.058]*	-0.3331[-0.069]**	-0.3283[-0.069]**	-0.3405[-0.071] **
		(0.0861)	(0.0406)	(0.0442)	(0.0376)
cert_CPA		0.1008[0.022]	0.06516[0.014]	0.09768[0.020]	0.1165[0.024]
		(0.4818)	(0.6613)	(0.5150)	(0.4395)
cert_CIA		0.03025[0.006]	0.02841[[0.006]	0.03786[0.008]	0.03345[0.007]
		(0.8334)	(0.8547)	(0.8078)	(0.8300)
LogExp_CAE		-0.1466[-0.031]	-0.2141[-0.045]**	-0.2292[-0.048]**	-0.2270[-0.049]**
		(0.1474)	(0.0396)	(0.0285)	(0.0311)
LogAge_IAF		-0.1274[-0.027]	-0.1872[-0.039]*	-0.1753[-0.037]*	-0.1740[-0.048] *
		(0.1914)	(0.0635)	(0.0832)	(0.0856)
LogSize_IAF		-0.004549[-0.0009]	-0.1056[-0.022]	-0.09979[-0.021]	-0.1008[-0.021]
		(0.9446)	(0.1463)	(0.1703)	(0.1670)
Budget		0.3761[0.080]***	0.2648[0.056]*	0.2530[0.053]*	0.2253[0.047]
		(0.0100)	(0.0796)	(0.0950)	(0.1406)
ACCountries		-0.03055[-0.007]	0.002683[0.0005]	0.006858[0.001]	0.02255[0.005]
		(0.8449)	(0.9867)	(0.9661)	(0.8897)
cert_IT	**H1a**		0.06156[0.013]	0.05120[0.011]	0.05919[0.012]
			(0.7578)	(0.7980)	(0.7676)
IT_Savvy_GEN	**H1b**		0.05978[0.013]	0.05180[0.011]	0.03894[0.008]
			(0.5411)	(0.5969)	(0.6934)
IT_Savvy_Data	**H1b**		0.4933[0.103]***	0.4635[0.097]***	0.4617[0.097]***
			(0.0000)	(0.0000)	(0.0000)
LogTraining_hours	**H1c**		-0.03282[-0.007]	-0.04915[-0.010]	-0.06218[-0.013]
			(0.8004)	(0.7053)	(0.6346)
Critical_Thinking	**H2**			0.1483[0.031]*	0.1267[0.027]
				(0.0521)	(0.2067)
Business_Savvy	**H3a**				0.01486[0.003]
					(0.8835)
Strategic_alignment	**H3b**				0.2504[0.052]
					(0.1135)
_cons		-0.6661*	0.08523	0.1257	0.03141
		(0.0853)	(0.8813)	(0.8259)	(0.9570)
LR chi2		16.60	65.49	69.30	71.95
		(0.1230)	(0.0000)	(0.0000)	(0.0000)
N		988	988	988	988
pseudo R-sq		0.0135	0.0534	0.0565	0.0587

Table 3.12 (Continued)

Percentage of Correctly Predicted (Goodness-of-fit) p-values in parentheses; Marginal Effect at Means in brackets	68.83%	69.13%	70.04%	70.34%
* p<.10	** p<.05	*** p<.01	**** p<.001	

The marginal effect at means shows that IAFs with sufficient budgets are 5.30% more likely to adopt big data analytics in support of business improvement processes than are IAFs with insufficient budgets. Moreover, it is evident from the analysis that for organizations belonging to the finance industry, that have experienced CAEs, and have matured IAFs tend not to adopt big data analytics in support of business improvement processes. These findings reflect on the strong corporate governance requirement that the use of IAFs be minimized/avoided for management operation ground; however, IAFs with sufficient budgets do tend to use big data analytics for business process improvement. These results suggest that when there are enough resources, IAFs might extend their use of data analytics to management operation ground even though such uses are discouraged by governance guidelines.

Table 3.13 (Equation 3) displays results for analysis of the adoption of data analytics in regulatory compliance. The analysis suggests that data-specific IT competencies (*IT_Savvy_Data*) and critical thinking skills (*Critical_Thinking*) are statistically significant in leading to the adoption of big data analytics in assuring regulatory compliance. Additionally, industry type is statistically significant, with IAFs in the finance or insurance industries having a 12.70% greater probability of adopting big data analytics than IAFs in other industries. Larger IAFs are also more likely to adopt big

data analytics in support of achieving regulatory compliance. The PCP of the model is 68.02%, indicating good fit.

Table 3.13

Regression Results and Marginal Effect at Means (Regulatory Compliance)

	Hypotheses	Model (1) DA_Assu_Reg	Model (2) DA_Assu_Reg	Model (3) DA_Assu_Reg	Model (4) DA_Assu_Reg
DA_Assu_Reg					
Size_Org		-0.08442[-0.02]***	-0.09967[-0.024]***	-0.1040[-0.025]***	-0.1014[-0.024]***
		(0.0073)	(0.0021)	(0.0015)	(0.0021)
LogAC_Meetings		-0.02561[-0.006]	0.08077[0.019]	0.05630[0.013]	0.05108[0.012]
		(0.9297)	(0.7908)	(0.8551)	(0.8693)
LogAC_IAF_Meetings		0.3013[0.072]	0.1236[0.029]	0.1522[0.036]	0.1648[0.039]
		(0.3072)	(0.6894)	(0.6265)	(0.6000)
Industry_Org		0.5397[0.128]****	0.5195[0.123]****	0.5379[0.127]****	0.5490[0.129]****
		(0.0002)	(0.0006)	(0.0004)	(0.0003)
cert_CPA		0.05988[0.014]	-0.01032[-0.002]	0.04898[0.012]	0.05713[0.014]
		(0.6665)	(0.9429)	(0.7374)	(0.6961)
cert_CIA		-0.09653[-0.023]	-0.1109[-0.026]	-0.09163[-0.022]	-0.08661[-0.020]
		(0.4909)	(0.4612)	(0.5457)	(0.5686)
LogExp_CAE		0.1457[0.035]	0.08225[0.019]	0.05994[0.014]	0.05822[0.014]
		(0.1379)	(0.4159)	(0.5565)	(0.5696)
LogAge_IAF		0.04593[0.011]	-0.01616[-0.004]	0.006266[0.0014]	0.002861[0.0007]
		(0.6295)	(0.8701)	(0.9498)	(0.9771)
LogSize_IAF		0.2053[0.049]***	0.1405[0.033]**	0.1555[0.037]**	0.1511[0.036]**
		(0.0013)	(0.0331)	(0.0199)	(0.0242)
Budget		0.1463[0.035]	0.03682[0.009]	0.01385[0.003]	0.01221[0.003]
		(0.3049)	(0.8039)	(0.9263)	(0.9353)
ACCountries		-0.3247[-0.077]**	-0.3081[-0.073]*	-0.3049[-0.072]*	-0.2846[-0.067]*
		(0.0342)	(0.0509)	(0.0551)	(0.0757)
cert_IT	**H1a**		-0.1532[-0.036]	-0.1717[-0.0405]	-0.1627[-0.038]
			(0.4402)	(0.3895)	(0.4157)
IT_Savvy_GEN	**H1b**		-0.04940[-0.012]	-0.06364[-0.015]	-0.06071[-0.014]
			(0.6041)	(0.5077)	(0.5310)
IT_Savvy_Data	**H1b**		0.5369[0.127]****	0.4893[0.115]****	0.4826[0.114]****
			(0.0000)	(0.0000)	(0.0000)
LogTraining_hours	**H1c**		0.1547[0.037]	0.1197[0.028]	0.1184[0.028]
			(0.2222)	(0.3472)	(0.3545)
Critical_Thinking	**H2**			0.2619[0.062]****	0.2483[0.057]**
				(0.0004)	(0.0115)
Business_Savvy	**H3a**				0.01439[0.003]
					(0.8822)
Fraud_DetRes	**H3c**				0.2552[0.060]
					(0.1449)
_cons		-1.2693****	-1.1286**	-1.0569*	-1.1281**

Table 3.13 (Continued)

	(0.0009)	(0.0435)	(0.0592)	(0.0467)
LR chi2	61.00	112.10	124.87	126.99
	(0.0000)	(0.0000)	(0.0000)	(0.0000)
N	988	988	988	988
pseudo. R-sq	0.0460	0.0846	0.0943	0.0959
Percentage of Correctly Predicted (Goodness-of-fit)	64.98%	67.51%	68.02%	66.60%
p-values in parentheses; Marginal Effect at Means in brackets				
* p<.10	** p<.05	*** p<.01	**** p<.001	

Table 3.14 (Equation 4) demonstrates results for the adoption of big data analytics in the detection of fraud or fraud risk management. The results suggest that when IAFs are assigned with fraud and risk management responsibilities (*Fraud_DetRes*), the likelihood of adopting big data analytics increases by 8.5%. Data-specific IT competencies (*IT_Savvy_Data*) are significant in the prediction of analytics use as well. It also appears that larger organizations (*Size_Org*) have a greater likelihood of adopting big data analytics. The model correctly classifies more than 65% of cases.

Table 3.15 (Equation 5) displays results for analysis of the adoption of big data analytics for risk control monitoring. The results for the adoption of big data analytics are similar to those of the adoption of data analytics in fraud risk management, with data-specific IT competencies (*IT_Savvy_Data*) and fraud risk responsibility (*Fraud_DetRes*) both statistically significant. Additionally, the size of the IAF is also statistically significant in predicting analytics use. Lastly, IAFs in Anglo-culture countries (*ACCountries*) are 7.02% more likely to adopt big data analytics in risk control monitoring than are IAFs in non-Anglo culture countries. The model correctly classifies 64.47% of cases.

Table 3.14

Regression Results and Marginal Effect at Means (Fraud Risk Management)

	Hypotheses	(1) DA_Assu_Fraud	(2) DA_Assu_Fraud	(3) DA_Assu_Fraud	(4) DA_Assu_Fraud
DA_Assu_Fraud					
Size_Org		0.06373[0.016]**	0.05889[0.014]*	0.05791[0.014]*	0.06065[0.015]*
		(0.0397)	(0.0759)	(0.0812)	(0.0709)
LogAC_Meetings		-0.4095[-0.101]	-0.2384[-0.059]	-0.2445[-0.059]	-0.2323[-0.057]
		(0.1374)	(0.4238)	(0.4136)	(0.4417)
LogAC_IAF_Meetings		0.5109[0.126]*	0.2480[0.061]	0.2552[0.063]	0.2662[0.065]
		(0.0692)	(0.4152)	(0.4031)	(0.3863)
Industry_Org		-0.2261[-0.056]	-0.3336[-0.082]**	-0.3316[-0.081]**	-0.3281[-0.080]**
		(0.1205)	(0.0339)	(0.0351)	(0.0381)
cert_CPA		0.02653[0.007]	-0.08693[-0.021]	-0.07069[-0.017]	-0.06364[-0.016]
		(0.8442)	(0.5538)	(0.6327)	(0.6676)
cert_CIA		0.1515[0.037]	0.1892[0.046]	0.1931[0.047]	0.1980[0.049]
		(0.2646)	(0.2183)	(0.2091)	(0.1992)
LogExp_CAE		-0.005496[-0.001]	-0.1046[-0.026]	-0.1102[-0.027]	-0.1213[-0.029]
		(0.9542)	(0.3130)	(0.2887)	(0.2467)
LogAge_IAF		0.02645[0.007]	-0.07095[-0.017]	-0.06590[-0.016]	-0.07539[-0.019]
		(0.7751)	(0.4790)	(0.5116)	(0.4545)
LogSize_IAF		0.1855[0.046]***	0.07355[0.018]	0.07833[0.019]	0.07296[0.018]
		(0.0045)	(0.2795)	(0.2507)	(0.2862)
Budget		0.2335[0.058]*	0.1036[0.025]	0.09846[0.024]	0.08365[0.021]
		(0.0954)	(0.4977)	(0.5197)	(0.5863)
ACCountries		-0.004804[-0.001]	0.01624[0.004]	0.01960[0.005]	0.03216[0.008]
		(0.9739)	(0.9186)	(0.9019)	(0.8411)
cert_IT	**H1a**		-0.1122[-0.028]	-0.1202[-0.029]	-0.1124[-0.028]
			(0.5806)	(0.5544)	(0.5818)
IT_Savvy_GEN	**H1b**		-0.1691[-0.042]*	-0.1728[-0.042]*	-0.1779[-0.044]*
			(0.0867)	(0.0804)	(0.0747)
IT_Savvy_Data	**H1b**		0.9819[0.241]***	0.9694[0.238]***	0.9705[0.238]***
			(0.0000)	(0.0000)	(0.0000)
LogTraining_hours	**H1c**		-0.03531[-0.009]	-0.04380[-0.011]	-0.05477[-0.013]
			(0.7802)	(0.7299)	(0.6680)
Critical_Thinking	**H2**			0.06869[0.017]	-0.008919[-0.002]
				(0.3429)	(0.9270)
Business_Savvy	**H3a**				0.1075[0.026]
					(0.2734)
Fraud_DetRes	**H3c**				0.3466[0.085]*
					(0.0587)
_cons		-0.8725**	0.2780	0.2960	0.2618
		(0.0180)	(0.6217)	(0.5995)	(0.6470)
LR chi2		35.42	172.58	173.48	178.08
		(0.0002)	(0.0000)	(0.0000)	(0.0000)
N		988	988	988	988
pseudo R-sq		0.0261	0.1272	0.1279	0.1313
Percentage of Correctly Predicted (Goodness-of-fit)		59.21%	68.22%	67.51%	66.40%

Table 3.14 (Continued)

p-values in parentheses; Marginal Effect at Means in brackets				
* p<.10	** p<.05	*** p<.01	**** p<.001	

Table 3.15

Regression Results and Marginal Effect at Means (Risk Control Monitoring)

	Hypotheses	Model (1) DA_Assu_ RCMoni	Model (2) DA_Assu_ RCMoni	Model (3) DA_Assu_ RCMoni	Model (4) DA_Assu_ RCMoni
DA_Assu_RCMoni					
Size_Org		0.01576[0.004] (0.6092)	0.007096[0.002] (0.8230)	0.005951[0.001] (0.8514)	0.007986[0.002] (0.8034)
LogAC_Meetings		-0.2050[-0.051] (0.4587)	-0.08870[-0.022] (0.7586)	-0.09831[-0.024] (0.7345)	-0.07751[-0.019] (0.7909)
LogAC_IAF_Meetings		0.1324[0.033] (0.6387)	-0.07767[-0.019] (0.7923)	-0.06848[-0.017] (0.8171)	-0.06481[-0.016] (0.8278)
Industry_Org		0.1096[0.027] (0.4504)	0.04539[0.011] (0.7627)	0.04893[0.012] (0.7451)	0.05242[0.013] (0.7292)
cert_CPA		-0.1242[-0.031] (0.3557)	-0.1971[-0.049] (0.1604)	-0.1763[-0.044] (0.2124)	-0.1675[-0.042] (0.2376)
cert_CIA		-0.1690[-0.042] (0.2112)	-0.1842[-0.046] (0.2087)	-0.1782[-0.044] (0.2247)	-0.1737[-0.043] (0.2386)
LogExp_CAE		-0.08872[-0.022] (0.3497)	-0.1693[-0.042]* (0.0869)	-0.1782[-0.044]* (0.0725)	-0.1910[-0.047]* (0.0563)
LogAge_IAF		0.05076[0.013] (0.5812)	-0.01698[-0.004] (0.8590)	-0.009164[-0.003] (0.9238)	-0.01846[-0.005] (0.8479)
LogSize_IAF		0.2470[0.061]*** (0.0001)	0.1619[0.040]** (0.0131)	0.1677[0.042]** (0.0105)	0.1615[0.040]** (0.0142)
Budget		0.1055[0.026] (0.4458)	-0.03447[-0.009] (0.8120)	-0.04201[-0.010] (0.7724)	-0.05940[-0.015] (0.6844)
ACCountries		0.2074[0.051] (0.1557)	0.2661[0.066]* (0.0798)	0.2697[0.067]* (0.0762)	0.2835[0.070]* (0.0647)
cert_IT	**H1a**		-0.06768[-0.017] (0.7250)	-0.07611[-0.019] (0.6928)	-0.06584[-0.016] (0.7336)
IT_Savvy_GEN	**H1b**		0.1015[0.025] (0.2686)	0.09663[0.024] (0.2928)	0.09116[0.023] (0.3260)
IT_Savvy_Data	**H1b**		0.4888[0.121]*** (0.0000)	0.4704[0.116]*** (0.0000)	0.4712[0.117]**** (0.0000)
LogTraining_hours	**H1c**		0.1007[0.025] (0.4092)	0.08861[0.022] (0.4690)	0.07640[0.019] (0.5353)
Critical_Thinking	**H2**			0.09629[0.024] (0.1714)	0.006549[0.0016] (0.9443)

Table 3.15 (Continued)

Business_Savvy	**H3a**				0.1266[0.031]
					(0.1792)
Fraud_DetRes	**H3c**				0.3654[0.091]**
					(0.0342)
_cons		-0.6669*	-0.2353	-0.2066	-0.2354
		(0.0686)	(0.6632)	(0.7024)	(0.6678)
LR chi2		31.23	94.12	96.00	102.06
		(0.0010)	(0.0000)	(0.0000)	(0.0000)
N		988	988	988	988
pseudo R-sq		0.0229	0.0691	0.0705	0.0749
Percentage of Correctly Predicted (Goodness-of-fit)		57.89%	63.06%	63.36%	64.47%
p-values in parentheses; Marginal Effect at Means in brackets					
* p<.10		** p<.05	*** p<.01	**** p<.001	

Overall, the results of multivariate analysis suggest that majority of hypotheses are supported, with the exception of training hours in IAFs and IAF alignment with organizational strategy. It might be case that training hours in IAFs are not specifically spent on data analytics, but perhaps are dedicated to more general auditing-related practices. Additionally, because of strong corporate governance practices, IAFs do not engage in activities that will jeopardize their objectivity and independence. Data-specific IT competencies (*IT_Savvy_Data*) are significant across all dependent variables, and it is confirmed that when IAFs face various management challenges, they are more likely to adopt big data analytics to cope with those challenges. Finally, IAFs in developed countries (particularly the Anglo-culture countries) are more likely to adopt big data analytics.

Additional Analysis

To document the interaction effects of significant variables, I calculated the marginal probabilities of adopting big data analytics. Figure 3.4 documents the interaction effects of the numerous significant variables predictive of the adoption of big data analytics for population testing rather than sampling. From Figure 3.4 (a), it is evident that, in small organizations, CAEs with a CPA certification are 8% more likely to adopt big data analytics than CAEs without CPA certification. Moreover, in large organizations, the conditional probability of adopting big data analytics by the IAF decreases in correspondence with the increase of the size of the organization, given that CAEs hold a CPA certification. This makes sense, since as the size of the organization increases, it is more likely to hire more personnel with data analytics competencies. In those cases, IT departments or data scientists might take provide support for data analytics. However, in small organizations it is evident that CAEs with CPA certifications play a critical role in the adoption of big data analytics for testing of populations rather than sampling. The same findings are true when the audit committee does not have a strong role [Figure 3.4 (b)] or when the size of the IAF is small [Figure 3.4 (c)]. In both cases, CAEs with CPA certifications are far more likely to adopt big data analytics for the testing of populations rather than sampling.

When data-specific IT competencies are low, CAEs with CPA certifications are more likely to adopt big data analytics, but with the increase of the data-specific IT competencies, the likelihood of CAEs with CPA certifications to adopt big data analytics decreases. This finding makes sense because IAFs might hire or train people with data analytics competencies who will serve to counteract lack of data-specific IT

competencies. The same finding is true for business savviness of IAFs [Figure 3.4 (d)]. Taken together, these findings suggest that in small organizations, or in the case of small IAFs, or when board oversight is not great, or when IAFs have low data-specific IT competencies, or when IAFs lack business knowledge, CAEs with CPA certifications are more likely to adopt big data analytics in the testing of populations rather than sampling.

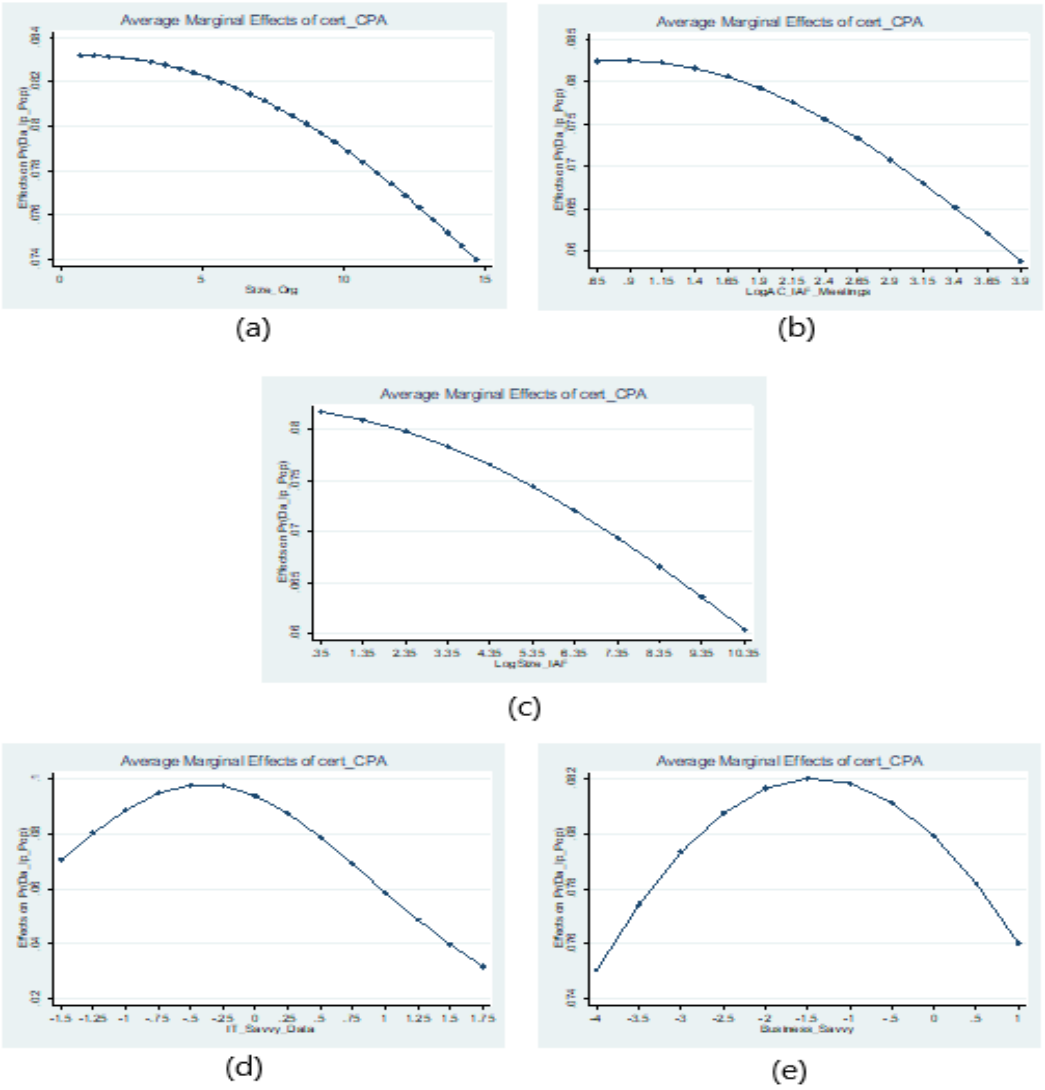


Figure 3.4 *Interaction Effects - Use of Data Analytics in Tests of Population Rather than Sample (DA_IP_Pop)*

Figure 3.5 highlights the interaction effects of sufficient budget and data-specific IT knowledge and critical thinking skills in the adoption of big data analytics in supporting business improvement processes. It is evident from Figure 3.5 (a) that when IAFs have sufficient budgets, they are about 3% more likely to adopt analytics given that their data-specific IT competencies remain the same. Moreover, when data-specific IT competencies increase, IAFs with sufficient budgets are 5.5% more likely to adopt big data analytics. Though overall adoption of data analytics in business process improvement is the lowest as I have seen in the descriptive statistics, it is evident that when IAFs have financial flexibility, they do tend to adopt big data analytics. The same scenario is true for IAFs with critical thinking skills [Figure 3.5 (b)]. IAFs with sufficient budgets are 4% more likely to adopt big data analytics in support of business improvement processes, given that both groups have similar critical thinking skills. It is evident that sufficient budgets allow IAFs either to hire data-knowledgeable personnel or to spend more on data-specific skills.

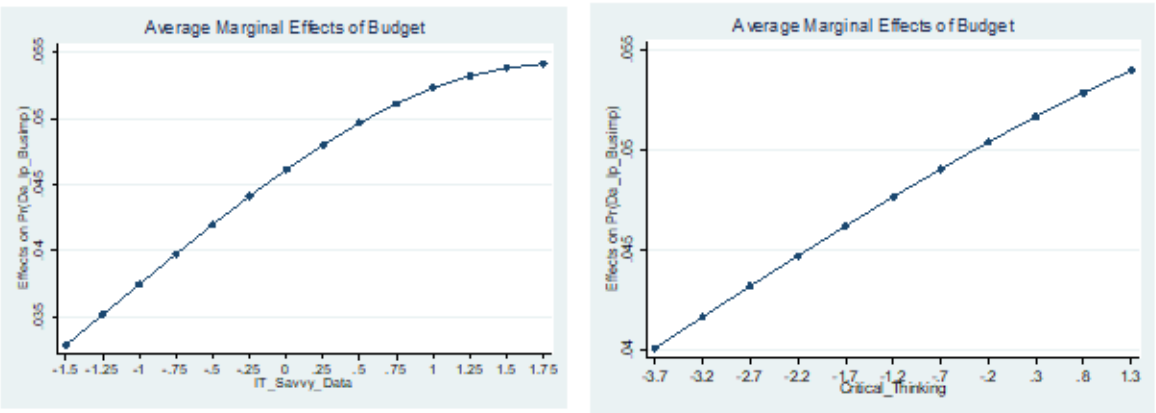


Figure 3.5 *Interaction Effects - Use of Data Analytics in Business Process Improvement (DA_IP_BusImp)*

It is evident from Figure 3.6 (a) that small IAFs in the finance industry are about 10.5% more likely to adopt big data analytics in support of monitoring regulatory compliance than IAFs that are not in finance industry. This finding confirms that when IAFs face management challenges, they are more likely to adopt big data analytics. Since, as established above, many organizations in the finance industry are required to use data analytics, this is an expected result. Given that IAFs have similar data-specific IT competencies [Figure 3.6(b)], IAFs in the finance industry are 9% more likely to adopt big data analytics in support of achieving regulatory compliance. The same finding is true in regard to critical thinking skills [Figure 3.6(c)]. Overall, these results confirm that when faced with greater management challenges, IAFs are far more likely to adopt big data analytics in order to cope with those challenges. This suggests that there may be an underutilization of big data analytics by auditors because of the lack of opportunity even though they may possess sufficient technical competencies.

When IAFs are challenged with fraud detection responsibilities, they are 7.4% more likely to adopt big data analytics for fraud risk management purposes, given that the organizations to which they belong are of the same size [Figure 3.7 (a)]. However, as the size of organization increases, this difference decreases; yet, IAFs with fraud detection responsibilities are still more likely to adopt big data analytics for fraud detection purposes. The reason for the decrease in probability with the increase in organizational size may be due to the ability of larger organizations to afford to employ data-savvy personnel which might serve to reduce the responsibility of IAFs in that regard. Similarly, IAFs with fraud detection responsibilities are more likely to adopt big data analytics given that they possess similar data-specific IT knowledge [Figure 3.7 (b)].

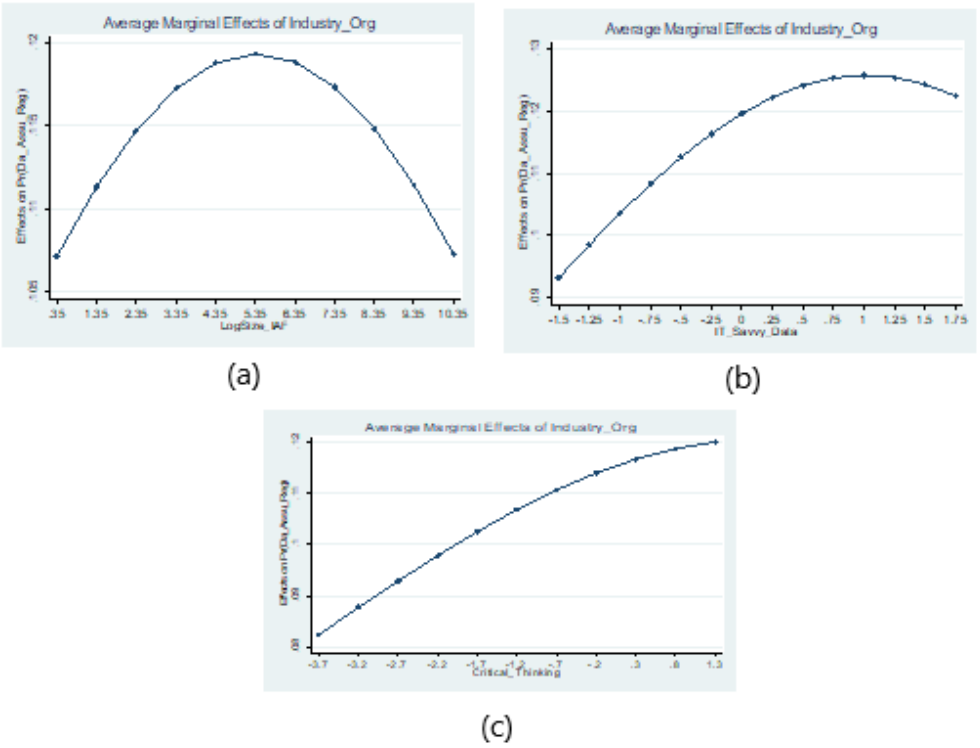


Figure 3.6 *Interaction Effects - Use of Data Analytics in Regulatory Compliance (DA_Assu_Reg)*

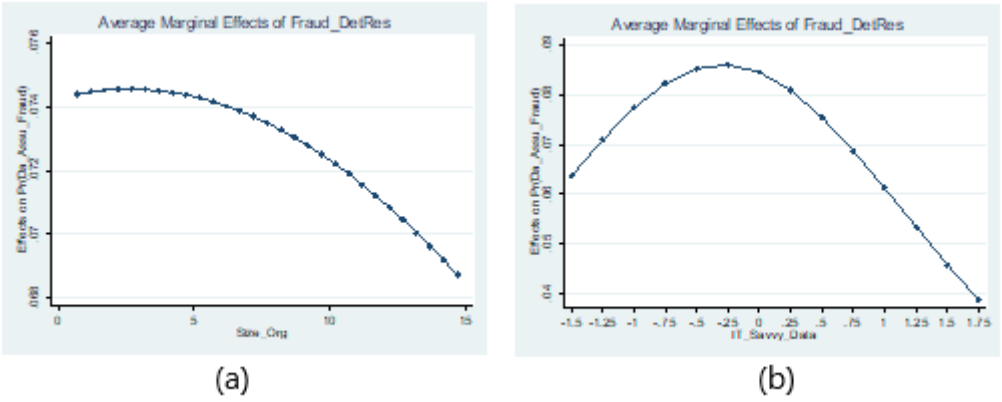


Figure 3.7 *Interaction Effects - Use of Data Analytics in Fraud Detection (DA_Assu_Fraud)*

Although the increase of data-specific IT knowledge decreases this probability, IAFs with fraud detection responsibilities are still more likely (about 4%) to adopt big data analytics for fraud risk management purposes. These findings further confirm that

when IAFs face management challenges, they are more likely to adopt big data analytics to deal with those challenges.

Figure 3.8 represents the analysis of big data analytics adoption for risk control monitoring in Anglo culture countries and when IAFs are tasked with fraud detection responsibilities. It is evident that, given similar IAF size, fraud detection responsibilities in Anglo culture country IAFs are more predictive of the likelihood of adopting big data analytics for risk control monitoring [Figure 3.8 (a)]. Even IAFs with fraud risk responsibilities in non-Anglo culture countries are more likely to adopt data analytics than IAFs with no fraud risk responsibilities in both Anglo and non-Anglo countries. These findings suggest that management challenges lead IAFs to adopt big data analytics, in general. The strong regulatory environment and effective implementation of corporate governance in Anglo countries might account for some of this. The same scenario holds when IAFs have same data-specific IT knowledge [Figure 3.8 (b)]. Taken together, the findings suggest that although data-specific IT knowledge is significant in the adoption of big data analytics, management challenges increase the probability of adopting big data analytics given that data-specific IT competencies are constant. The difference of the probability for adopting the data analytics remains the same even if data-specific IT knowledge increases.

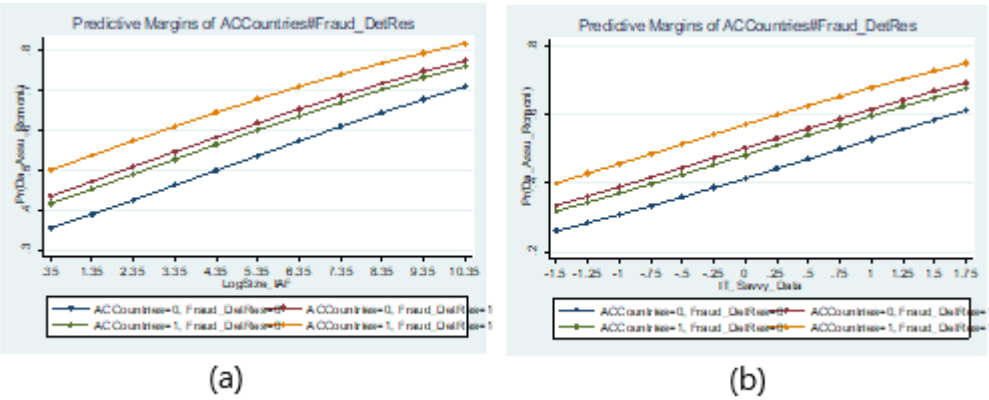


Figure 3.8 *Interaction Effects - Use of Data Analytics for Risk Control Monitoring (DA_Assu_RCmoni)*

Overall, the results from the analysis of interaction effects provide deeper insights about the adoption of big data analytics by IAFs. CAEs with CPA certifications are more likely to adopt big data analytics in small organizations, or in small internal audit departments, or when board involvement is low, or even when there are low IT and business skills. Further, an IAFs' resources (such as sufficient budget) can also account for the adoption of big data analytics. Additionally, IAFs in highly-regulated environments such as the finance industry are more likely to adopt big data analytics. Finally, when IAFs are tasked with fraud risk management responsibilities, they are far more likely to adopt big data analytics in Anglo culture countries given that they have same data-specific IT knowledge, are part of similar-sized organizations, and are of similar departmental size. These findings, taken together, indicate that although data-specific IT knowledge, or CPA certifications, or sufficient budgets have an impact on data analytics adoption, management challenges such as operation in highly regulated industries or fraud risk management responsibilities increase the probability of the adoption of data analytics given that IAFs have similar competencies or similar size.

Discussion and Conclusion

Given the availability of the increasingly unprecedented amount of data in modern business, organizations in all industries have already begun capitalizing on the availability of data for achieving competitive advantages, thus improving ROA, asset utilization, and market value. This scenario of their clients also puts the burden on accountants/auditors to similarly embrace big data analytics. Data analytics have the potential to fundamentally change accounting and auditing processes such as infer (insight), predict (foresight), and assure (oversight) tasks performed by auditors/accountants (Schneider et al. 2015). However, there remain significant challenges to be overcome for accountants to reap the benefits of analytics technologies (Earley 2015). In particular, three kinds of challenges are documented in the literature – data (skill) challenges, process (cognition) challenges, and management (organization) challenges.

Data challenges are related to data-specific technical knowledge. It is evident that there are shortages of data-savvy personnel in accounting/auditing. This shortage arises from two primary reasons– one is the lack of data scientists in the market (supply) and the other is the demand for such data scientists by all kinds of organizations (demand). Process (cognition) skills are related to the evaluation of vast amounts of data. Although big data analytics have significant potential to improve the judgment and decision-making processes of accountants/auditors, it also brings with it the risk of introducing biases in the decision-making process. Big data might also overwhelm accountants since it requires a very high tolerance for ambiguity. Therefore, accountants/auditors are in need of high process (cognition) knowledge. Sometimes accountants/auditors also face

challenges from their own organization or industry. It is suggested that having knowledge about data analytics alone will not create the benefits for accountants unless they have good knowledge about their businesses they serve (Richins et al. 2017). So, accountants need both data analytics skills and domain-specific business knowledge. Moreover, sometimes accountants' responsibilities such as fraud detection and risk management or business process improvement might motivate accountants to adopt big data analytics because of its enormous potential to deal with those challenges.

The purpose of this research is to study accountants' adoption of big data analytics in their work processes, including procedures such as the testing of populations, business process improvements, assurance of regulatory compliance, risk control monitoring, and fraud risk management. The results of the study indicate that data-specific IT knowledge of IAFs is central in explaining the adoption of big data analytics to support the work processes of accountants. Even though many IAFs are have acceptable general IT knowledge, this general knowledge does not account for the adoption of data analytics. As such, accountants are encouraged to focus on improving data-specific IT knowledge in order to reap the benefits of big data analytics. Additionally, the critical thinking skills of IAFs (e.g., process knowledge) and business savviness are also significant predictors. Taken together, these findings support the influence of both technical competencies (hard knowledge) and process and business knowledge (soft knowledge) which are required for accountants to fully appreciate and effectively utilize big data analytics. When IAFs are in highly regulated industries or when IAFs are tasked with fraud risk management responsibilities, they are more likely to adopt big data analytics in their work process. Sometimes, resources such as

sufficiency of budgets also play a role in the adoption of data analytics. However, it is found that the adoption of big data analytics by IAFs for business process improvement is limited, implying that accountants might be unwilling to use IAFs for management operation ground.

The results of the research further our understanding of the adoption and subsequent usage of big data analytics when additional analysis (i.e., interaction effects) is performed on the significant variables. The presence of CAEs with CPA certifications in the firm is significant in explaining the adoption of data analytics. In particular, in the case of CAEs with CPA certifications in small organization, or in small IAFs, or when there is reduced board oversight, or when there is a lack of data-specific IT knowledge or business knowledge, adoption likelihood is increased as compared to situations with CAEs who have no CPA certifications. These findings suggest that small organization, or small internal audit departments, should consider employing CAEs with CPA certifications even if there is a lack of data-specific IT knowledge or business knowledge.

It is also found that when IAFs have sufficient budget, they are more likely to adopt big data analytics in support of business improvement processes even if they lack data-specific IT knowledge or critical thinking skills. This suggests that IAFs will seek to use data analytics for management operations only when they have sufficient organizational slack. Further, IAFs in organizations operating in the finance industry are more likely to adopt data analytics than other IAFs even when both groups have the same size, enjoy similar data-specific IT competencies, and possess process knowledge - thus indicating that management challenges in many cases lead accountants to adopt big data analytics. Similar findings are documented when IAFs are tasked with fraud detection

responsibilities. These findings, taken together, support the conclusion that when two IAFs have the same technical and process knowledge, the IAFs with additional management challenges are more likely to adopt big data analytics. This conclusion stems from the fact that big data analytics provide the ability to deal with the challenges that accountants face in their normal work process. Finally, when comparing IAFs in Anglo culture countries to IAFs in non-Anglo culture countries, given the same size and technical competencies, it is found that IAFs with fraud risk responsibilities in Anglo culture countries have the higher probability of adopting big data analytics than other IAFs. In sum, these findings suggest that IAFs in developed countries are more likely to adopt big data analytics given that they are on the same footing with their non-Anglo counterparts.

As with all empirical survey investigations, the study has some limitation. The items to measure latent constructs might not fully represent the constructs, there being no previously-validated scale for the items related to data analytics in the literature. Moreover, for dependent variables, a few but representative areas in which internal auditors can apply big data analytics have been represented; there are most surely others that can be assessed, as well. There might also be other inhibitors associated with incorporating big data into accounting that the study could not incorporate.

Even so, the findings of the study have both theoretical and practical implications. The findings contribute to the literature in several ways. First, the results of the study provide empirical support for the assertion that the challenges to big data analytics have implications for improving accounting practice. Second, the study highlights the respective role of each challenge. Particularly, the results suggest that data-specific IT

knowledge is the most significant factor in supporting the adoption of data analytics. Therefore, accountants should focus on how they can improve their technical competencies for data analytics. Moreover, the results suggest that not only technical competencies but also process knowledge and business domain-specific knowledge leads accountants to adopt data analytics. It is evident that when two IAFs have same technical or process knowledge, IAFs with added management challenges such as increased regulation and fraud risk management responsibilities are more likely to adopt big data analytics than IAFs without such management challenges. From a practical standpoint, the findings of the study demonstrate how small organizations or small IAFs can improve the usage of big data analytics by employing CAEs with specialized knowledge such as CPA certifications. Secondly, the research will better inform the external auditing process in its evaluation of the decision to rely on the work product of internal auditors simply by highlighting the factors that are significant in IAF reliance on big data.

CHAPTER 4

OUTSOURCING OF BIG DATA ANALYTICS BY INTERNAL AUDIT FUNCTION (IAF)

Introduction

The omnipresent availability of vast amounts of data provides great opportunities for improving the bottom line of organizations. Regulators are also increasingly encouraging organizations to use data. However, the real value of data arises from the analytics applied to the data. Not only can organizations reap the benefits of big data analytics, data analytics have the potential to fundamentally change the auditing and accounting task processes (Schneider et al. 2015). Big data analytics have great potential to provide better forecasting estimates, support going concerns, detect instance of fraud, and other business factors are of interest to auditors (Alles 2015). Given these perspectives, accounting academics are focusing on different issues related to the adoption and use of big data analytics in the accounting/auditing profession.

In this research, I focus on the outsourcing of big data analytics by the Internal Audit Function (IAF) of organizations. Of external and internal auditors, IAFs have a greater likelihood than external auditors to use big data analytics because the scope of work for IAFs is much broader than that of external auditors. IAFs also have easy access to organizational data, and the work of IAFs is not overly regulated as is the case with external auditors. Studying the outsourcing of big data analytics by auditors is important

because the same individuals (IAFs) who provide data for outsourcing data analytics will also be directly affected by the outcome of those outsourcing decisions and must rely on the work performed by the service organizations[9] , which are engaged in the outsourcing process. Thus, the motivations of accounting personnel who provide the financial inputs for organizational analytics are relevant and must be carefully considered when choosing the appropriate outsourcing solution (Christ, Mintchik, et al. 2015).

Blaskovich and Mintchik (2011, 13) suggest that "the complexity of the Information Technology Outsource (ITO) choice demands additional investigation of the sociologic, strategic, and economic factors that determine the decision. Although research on these drivers has been conducted for several decades, the dynamic nature of technology continues to raise interesting questions and offer fruitful avenues for research." Christ et al. (2015) also noted that in the Outsourcing of Information Systems (OIS)[10], big data analytics outsourcing and IT outsourcing are not identical business practices. Therefore, accounting scholars should exercise caution and evaluate the similarity of contextual factors when considering whether to extrapolate the wealth of general IT outsourcing findings in the literature to the particular context of big data analytics outsourcing. As a further context-specific complication, in considering general IT outsourcing wisdom in the context of specific analytics outsourcing objectives, outsourced accounting functions must be performed in specific compliance with regulatory requirements, are subject to external monitoring by regulatory authorities, and

[9] Service organizations are those who will provide data analytics service; user organizations are those who will outsource data analytics. In this case, IAFs are user organization.

[10] For General outsourcing (Including IT outsourcing), accounting function primarily provides financial and performance data used to evaluate new or ongoing outsourcing relationships. Alternatively, when companies engage in OIS, the accounting function not only provides the input for the decision process, the accounting function itself is fundamentally changed as a result of OIS.

may also result in sanctions and significant penalties for non-compliance. Hence, the outsourcing of big data analytics by IAFs warrants careful investigation. A shared understanding of the business rationale for outsourcing alliances and the use of measurable objectives to monitor the performance of such alliances are crucial factors for long-term success; therefore, insights into user organization motivations for outsourcing big data analytics can help practitioners identify the appropriate control practices for OIS relationships in remediation of the associated risks (Christ, Mintchik, et al. 2015).

Since there is little research on OIS in accounting contexts (Christ, Mintchik, et al. 2015), one must draw upon the literature from areas outside of accounting. The literature on outsourcing identifies three disciplines that explain the outsourcing decision-making process. These disciplines include economics, strategy, and sociology. Transaction Cost Economics (TCE) and Agency Theory (AT) from economics posit that companies are more likely to outsource services that are common, frequently performed, and rarely changed. The strategic perspective from management posits that outsourcing arises from a decision to focus on core competencies, from concerns about in-house capabilities, from opportunities for restructuring, and/or from a desire to access technology and expertise (Christ, Mintchik, et al. 2015). Researchers propose that strategic drivers will dominate cost considerations when outcomes are unpredictable or when there are significant organizational changes. The sociological perspective suggests that there exists a broad array of relationship-driven motivations to engage in OIS. For example, because Sarbanes Oxley Act (SOX) requires US executives to personally certify that internal controls are effective, and the financial statements are fairly stated, executives might prefer to outsource subjective processes, such as the preparation of

complex estimate in an attempt to distribute responsibility and to make the estimates more justifiable.

The results of this study suggest that, contrary to conventional wisdom, economic factors as represented by the sufficiency of the budgets allocated to IAFs are not significant predictors of outsourcing of audit functions. Rather, strategic and sociological factors are most indicative of the likelihood of outsourcing big data analytics. Specifically, IAFs outsource big data analytics when they lack data skills to perform the processes and when they are tasked with fraud risk management responsibilities. Additionally, the role Chief Audit Executives (CAEs) is also significant. There is also a cultural variation of the outsourcing decision; IAFs from developing nations are more likely to outsource than are IAFs from developed countries. Further analysis of the interaction effects of these significant variables suggests that as the data skills of IAFs increase, the conditional difference of the likelihood of outsourcing decreases, suggesting that IAFs recognize both the value of data analytics and their related lack of competencies. The three-way interactions of the variables support the same conclusion.

This study contributes to the literature in several ways. First, since outsourcing involves risks, appropriate controls are required to mitigate risks and insights into user organizations' motivations for outsourcing can help in identifying the appropriate control practices for outsourcing relationships (Christ, Mintchik, et al. 2015). Second, contrary to previous expectations that companies are more likely to outsource services that are common, and which are rarely changed, the study provides evidence that this conventional wisdom does not apply for all situations related to the outsourcing of auditing analytics. Third, the findings also provide guidance for external auditors when

they evaluate the objectivity and competence of IAFs before relying on their work. These findings add to our understanding about the role of accountants in outsourcing in response to calls in the literature for understanding the role of accountants and auditors in the IT outsourcing process.

Theoretical Background and Hypotheses Development

Accounting information systems practice is intertwined with Information Technology (IT) infrastructure; yet, there is little research by accounting academics on the outsourcing of IT functions by accountants or auditors (Christ, Mintchik, et al. 2015; Blaskovich and Mintchik 2011). Therefore, accounting researchers default to the reference disciplines to explore the determinants of outsourcing of accounting functions. The literature identifies three categories of determinants for IT outsourcing: economic, strategic, and sociologic. Transaction Cost Economics (TCE) posits that organizations usually outsource in order to minimize costs. Specifically, organizations weigh both production costs and contracting costs before making outsourcing decisions. TCE postulates that organizations tend to outsource those activities that are common, frequently performed, rarely changed, and have easily measurable quality (Christ, Mintchik, et al. 2015). Firms with a lack of financial slack also tend to outsource (Smith, Mitra, and Narasimhan 1998; Hall 2005).

Obtaining personnel trained in big data analytics is one of the greatest obstacles in accounting (Alles, 2015), exacerbating the possibility of building in-house capabilities. IAFs find it very difficult to compete for big data talent since most competitors are also vying for analytics personnel. Research indicates that many auditors consider financial resources a barrier to the adoption of data analytics (Protiviti 2017). Historically, long

term financial flexibility affects the adoption of audit software by auditors and surveys document that a very small amount of financial resources have been dedicated to data analytics by auditors (Protiviti 2017). Given this reasoning and circumstances, it is hypothesized that:

H1*: IAFs with sufficient financial resources are more likely to outsource big data analytics.*

Many researchers charge that the economic perspective of outsourcing is too narrow and subsequently depicts a short-term perspective. For that reason, some scholars draw upon strategic theories to account for outsourcing decisions. Strategic theory postulates that outsourcing arises from the decision to focus on core competencies, concerns about in-house capabilities, opportunities for restructuring, and a desire to access technology and expertise (Christ, Mintchik, et al. 2015). In this view, anything that did not contribute immediately to the characteristics that directly support the competitive bottom line would be outsourced in order to free up organizational slack for concentration on competitive objectives.

Researchers postulate that when outcomes are unpredictable or when there are significant organizational changes underway, strategic theories prevail over cost considerations in organizational decision-making. Since big data analytics has the potential to fundamentally change the nature of the work of accountants in the firm, it may lead to competitive advantages and a related desire to develop in-house capabilities and skills for data analytics. Alternatively, if accountants cannot develop in-house capabilities, in view of the growing recognition of the importance of analytics in

accounting and auditing, they might tend to outsource the analytics process to gain access to necessary skills and technologies. Therefore, it is hypothesized that:

H2*: Data analytics skills of IAFs are negatively associated with the outsourcing.*

Some researchers contend that sociological motivations of different roles in organizations are also important for understanding the behavior of outsourcing aspects of the accounting function. Generally, this line of research focuses on the effects of relationships among companies and/or individuals on outsourcing decisions (Christ, Mintchik, et al. 2015). The nature of such relationships is affected by organizational politics, power, contracting, institutionalism, institutional isomorphism, and social norms. Blaskovich and Mintchik (2011) noted that sociological motivations for outsourcing arise from a political power struggle with chief IT personnel, pressure from IT vendors, and related factors.

The jobs and responsibilities of accountants are defined by numerous regulations and corporate governance guidelines specific to particular industries. These circumstances might shape interplay of power and politics, thus affecting the decisions on outsourcing. For example, many financial organizations require that every audit use data analytics or that auditors validate that they reviewed their scope and approach for data analytics use and justifies why analytics were be used (Protiviti 2017). Further, because of the requirements of Sarbanes Oxley, accounting executives might prefer to outsource subjective processes in an attempt to distribute responsibility and to make potentially risky decisions appear more justifiable (Christ, Mintchik, et al. 2015).

Research suggests that executives related to IT play leading roles in the consideration of outsourcing but that final decisions are often made by a small number of

business executives with little IT knowledge (Sobol and Apte 1995). In IAFs, Chief Audit Executives (CAEs) are the managers who makes strategic decisions (such as the adoption of big data analytics) and it is acknowledged that different kinds of certifications held by CAEs reflect on their specialized knowledge. Since big data analytics demands special knowledge, it is expected that CAEs with certifications might play a critical role in the data analytics outsourcing or usage decision. Tang et al. (2017) documented that the Certified Public Accountant (CPA) certification is the one most commonly found in IAFs. Therefore, it is hypothesized that:

H3*: Chief Audit Executives (CAEs) with CPA certifications tend to outsource big data analytics.*

Another important sociological aspect that might have an effect on outsourcing decisions in the auditing function is corporate governance practice. Specially, the role of the audit committee is important because IAFs report to them and since audit committee is charged with the overall financial responsibility of organizations. Since big data analytics has greater potential to streamline the operations of accountants, persons responsible for corporate governance such as the audit committee might play a critical role in gaining access to this emerging technology. Research also documents that audit committees play a critical role in the adoption of emerging technologies and process (Abdolmohammadi et al. 2017; Islam, Farah, and Stafford 2018). Therefore, it is hypothesized that:

H4*: Audit Committee oversight will be positively associated with the outsourcing decisions for big data analytics.*

Of the many applications in which data analytics can be employed by accountants, fraud detection is increasingly important. Regulators such as the Securities and Exchange Commission (SEC) also use big data analytics to identify fraud in financial statements and to identify audit failures. Fraudulent insurance claims are also detected by auditors using big data analytics. In most of the organizations, IAFs are tasked with the responsibility for fraud detection; for these reasons it is hypothesized that:

H5*: IAFs with fraud detection responsibility is more likely to outsource big data analytics.*

The outsourcing literature suggests that country characteristics might affect the extent and the form of IT outsourcing (Apte et al. 1997). Members of the accounting practice suggest that culture represents a major barrier to the successful implementation of analytics (Protiviti 2017). The oversight of corporate governance personnel also might not be as rigorous in developing countries as in developed ones, which could lead to overlooking the potential of big data analytics in risk control monitoring, risk assessment, fraud detection, and regulatory compliance. Therefore, it is expected that the outsourcing of data analytics by IAFs will vary from culture to culture. Because of the shortage of personnel skilled in data analytics and owing to a distance barrier in acquisition of such personnel, IAFs in developing nations will tend to outsource data analytics. As such, it is hypothesized that:

H6*: IAFs from developing countries are more likely to adopt big data analytics than are IAFs from developed countries.*

Research Methodology

Sample

The data for the study were collected from the Common Body of Knowledge database (CBOK 2015) developed by The Institute of Internal Auditors Research Foundation (IIARF). For the study, only the responses from Chief Audit Executives (CAEs) were used, on the rationale that they are more knowledgeable and experienced than the balance of personnel in the internal audit department. The distribution of the data is given in Table 4.1 to Table 4.3.

Table 4.1

Distribution of Sample (Number of Observations)

Total Respondent	14518
Less: Director or Senior Manager	1630
Less: Manager	2098
Less: Staff	5644
Less: Missing Value for Respondents' Position	182
Less: Academic Staff or Retired	1620
Chief Audit Executives (CAEs)	3344
Less: Missing Values for Dependent & Independent Variables	2928
Total Observations Used	**416**

Table 4.2

Distribution of Sample (Types of Organizations)

Type_Org	Freq.	Percent	Cum.
Privately Held	137	32.93	32.93
Publicly Traded	160	38.46	71.39
Public Sector	85	20.43	91.83
Not for Profit	24	5.77	97.60
Other	10	2.40	100
Total	416	100	

Table 4.3

Distribution of Sample (Regions Represented)

Region_Org	Freq.	Percent	Cum.
Africa	44	10.58	10.58
Asia	72	17.31	27.88
Europe	123	29.57	57.45
Latin America	51	12.26	69.71
North America	115	27.64	97.36
Oceania	11	2.64	100
Total	416	100	

Variable Measurement and Empirical Model

The dependent variable of the study is the percentage of data analytics activities that IAFs outsource. For hypothesis **H1**, the financial flexibility of IAFs is represented by the amount of budget they receive from the organization. Budget is a dummy variable (*Budget*), with one representing IAFs that have completely sufficient budgets or zero otherwise. For **H2**, data analytics skills of IAFs (*IT_Savvy_Data*) are measured by factor scores; to calculate factor scores, Bartlett method was used. Exploratory factor analysis using principal components produced one factor with the eigenvalues greater than 1, and this factor accounts for 67.84% of variance. The items and factor loadings are displayed in Table 4.4 and Table 4.5 respectively. All factor loadings are above the threshold recommended by Hair et al. (1998). For **H3**, CAEs with CPA certifications is measured using a dummy variable (*cert_CPA*), with one representing CAEs who hold a CPA certificate, zero otherwise. For hypothesis **H4**, audit committee oversight was measured using the log of the number of audit committee or equivalent meetings in which CAEs were invited to attend (*LogAC_IAF_Meetings*).

Table 4.4

Items to Measure Latent Construct

IT_Savvy_Data	What is the extent of activity for your internal audit department related to the use of the following IT tools and techniques? 1 = None; 2 = Minimal; 3= Moderate; 4= Extensive 5. A software or tool for data mining (ITSD1) 6. An automated tool for data analytics (ITSD2) 7. Computer Assisted Audit Technique (ITSD3) 8. Continuous/Real time Auditing (ITSD4)

Table 4.5

Factor Loadings (Principal Component Factor with Varimax Rotation)

Items	IT_Savvy_Data
ITSD1	**0.8175**
ITSD2	**0.8766**
ITSD3	**0.8197**
ITSD4	**0.7778**

The auditing literature frequently uses the number of meetings held by the audit committees to measure the oversight of the audit committee in the organization. The fraud detection responsibility (**H5**) is measured using a dummy variable (*Fraud_DetRes*), with one representing IAFs who have all or most of the responsibility to detect fraud in the organization or zero otherwise. Studies that use the CBOK (2015) database usually consider Anglo-culture countries developed countries. In line with the literature and expectations, developing countries (**H6**) is measured by using a dummy variable (*Non_ACCountries*), with one representing the IAFs not belonging to UK/Ireland, USA, Canada, Australia, New Zealand, or South Africa, zero otherwise. Additionally, several control variables were included, but when Full Model (FM), including the controls, is

run, all of the controls were insignificant. Therefore, the Reduced Model (RM) was used for hypothesis testing. The empirical model of the study is:

$$Prob\ (Ousource\_DA) = F\ [\alpha_0 + \alpha_1\ Budget + \alpha_2\ IT\_Savvy\_Data + \alpha_3\ cert\_CPA + \alpha_4\ LogAC\_IAF\_Meetings + \alpha_5\ Fraud\_DetRes + \alpha_6\ Non\_ACCountries] + \boldsymbol{\varepsilon} \quad \text{Eq. (4.1)}$$

Since the response variable (*Ousource_DA*) is a fraction, including both zero and one, it is recommended that Fractional Regression (FR) rather than Ordinary Least Squares (OLS) or Beta Regression (BR) be utilized in analysis (Liu and Xin 2014; Dorta 2016).

Results

Descriptive Analysis of Variables

Summary statistics in Table 4.6 shows that, on average, 20% of data analytics activities are outsourced by IAFS, but the standard deviation (23%) is greater than the mean indicating that there is a lot variation in the outsourcing of data analytics. Of the outsourcing organizations, privately-held and not-for-profit outsource most (23%), followed by public sector firms. Publicly-traded organizations outsource the least (17%). There is no statistical difference between organizations in term of data analytics outsourcing ($p < 0.21$).

A little more than 33% of IAFs, on average, have sufficient budgets to support analytics and the difference is not significant across organization types ($p < 0.33$). The average value of data analytics skills is 0, with the standard deviation being 1. This finding is in line with the Bartlett factor scores, since the Bartlett method standardizes the responses with a mean of one and a standard deviation of 1.

Positive factor scores indicate skills above the average and negative factor scores indicate skills below the average. Though there are both positive and negative factor scores for the variable *IT_Savvy_Data*, the difference across the type of organization is not statistically significant ($p < 0.27$). Further, on average, 46% CAEs have CPA certifications, with the difference across the organization type being statistically insignificant ($p < 0.52$). However, the difference in audit committees' oversight is not significant ($p < 0.45$). Only 25% of IAFs are responsible for fraud detection, with the difference being insignificant ($p < 0.65$), while the outsourcing decision is significant across organizations in terms of culture ($p < 0.00$), suggesting that culture has a bearing on outsourcing decisions.

Table 4.6

Summary Statistics of Variables Across Different Types of Organizations

	Full Dataset	Privately Held	Publicly Traded	Public Sector	Not for Profit	Other	F-Stat/ $\chi 2$ (Sig)
Outsource_DA	0.20	0.23	0.17	0.19	0.23	0.18	1.48
	(0.239)	(0.253)	(0.227)	(0.216)	(0.292)	(0.268)	(0.21)
Budget	0.34	0.34	0.38	0.26	0.38	0.50	4.60
	(0.476)	(0.476)	(0.486)	(0.441)	(0.495)	(0.527)	(0.33)
IT_Savvy_Data	0.00	0.29	0.04	-0.20	-0.10	-0.10	1.30
	(1.00)	(0.983)	(0.983)	(1.015)	(1.039)	(0.978)	(0.27)
cert_CPA	0.46	0.42	0.45	0.48	0.58	0.60	3.23
	(0.499)	(0.496)	(0.499)	(0.503)	(0.504)	(0.516)	(0.52)
LogAC_IAF_Meetings	1.65	1.59	1.71	1.64	1.70	1.53	3.72
	(0.527)	(0.536)	(0.511)	(0.545)	(0.545)	(0.400)	(0.45)
Fraud_DetRes	0.25	0.21	0.25	0.27	0.25	0.40	2.45
	(0.431)	(0.410)	(0.434)	(0.447)	(0.442)	(0.516)	(0.65)
Non_ACCountries	0.67	0.80	0.64	0.62	0.21	0.80	34.91
	(0.471)	(0.405)	(0.480)	(0.487)	(0.415)	(0.422)	(0.00)
N	416	137	160	85	24	10	

Multivariate Analysis and Tests of Hypotheses

The correlation matrix in Table 4.7 suggests all correlations are below 0.5 and the relationship between outsourcing, and fraud detection and culture are significant, thus

supporting H5 and H6. Several other relationships between explanatory variables are also significant. Table 4.8 contains the results of Factorial Regression (FG) analysis and suggests that data analytics skills of IAFs have significant negative relationships with outsourcing decisions, indicating that if the data analytics skills of IAFs increase, they tend not to outsource. This finding confirms the expectation that IAFs either prefer focus on core activities or that they are concerned about the lack of pertinent skills when they have low data analytics capabilities. CAEs with CPA certifications played an important role in outsourcing decisions, and IAFs with fraud detection responsibilities were also more likely to outsource (H5). Finally, IAFs from developing countries are more likely to outsource. However, no support is found for cost considerations or audit committee oversight. Since the coefficients of Fractional Regression (FR) are difficult to interpret, the marginal effects at means (which measure the change in the response variable for the change in an explanatory variable holding other variable values at means), are also included. For example, marginal effect at means for *Fraud_DetRes* indicates that IAFs with such responsibilities are 5.3% more likely to outsource than IAFs without such responsibility.

Table 4.7

Correlation Matrix

	1	2	3	4	5	6	7
1.Outsource_DA	1						
2.Budget	-0.0678	1					
3.IT_Savvy_Data	-0.0893	0.1370**	1				
4.cert_CPA	0.0512	0.0441	0.0940	1			
5.LogAC_IAF_Meetings	-0.0058	0.00330	0.1670***	0.0234	1		
6.Fraud_DetRes	0.0984*	-0.0007	0.1060*	-0.0654	-0.0689	1	
7.Non_ACCountries	0.120*	-0.0598	-0.0805	-0.201***	-0.0642	0.1290**	1

Table 4.8

Regression Results and Marginal Effects at Means

	Outsource_DA	Marginal Effect at Means
Outsource_DA		
Budget	-0.171	-0.0268
	(-1.06)	(-1.06)
IT_Savvy_Data	**-0.145***	-0.0227*
	(-1.81)	(-1.79)
cert_CPA	**0.276***	**0.0433***
	(1.87)	**(1.86)**
LogAC_IAF_Meetings	0.0641	0.0100
	(0.48)	(0.48)
Fraud_DetRes	**0.339****	**0.0530****
	(2.10)	**(2.11)**
Non_ACCountries	**0.391****	**0.0613****
	(2.15)	**(2.19)**
_cons	-1.94****	
	(-6.73)	
N	416	416

* p<.10 ** p<.05 *** p<.01 **** p<.001

Additional Analysis

The interaction effects of significant variables are presented in Figure 4.1 and 4.2. Figure 4.1(a) shows that when IAFs data analytics skills are low, IAFs from the developing nations are 7% more likely to outsource big data analytics than IAFs from developed countries. As the skills increase, the difference decreases, indicating that IAFs consider big data analytics a core skill. Further, when IAFs have low data analytics skills but are assigned fraud detection responsibilities, they are 6% more likely to outsource big

data analytics (Figure 4.1(b)). The same scenario holds for the other variables. Taken together, the findings suggest that IAFs consider data analytics to be a critical skill and that they only outsource when they are low in data analytics skills, but the likelihood of outsourcing decreases as the skills increases. This tends to validate the strategic perspective of outsourcing in IAF decisions.

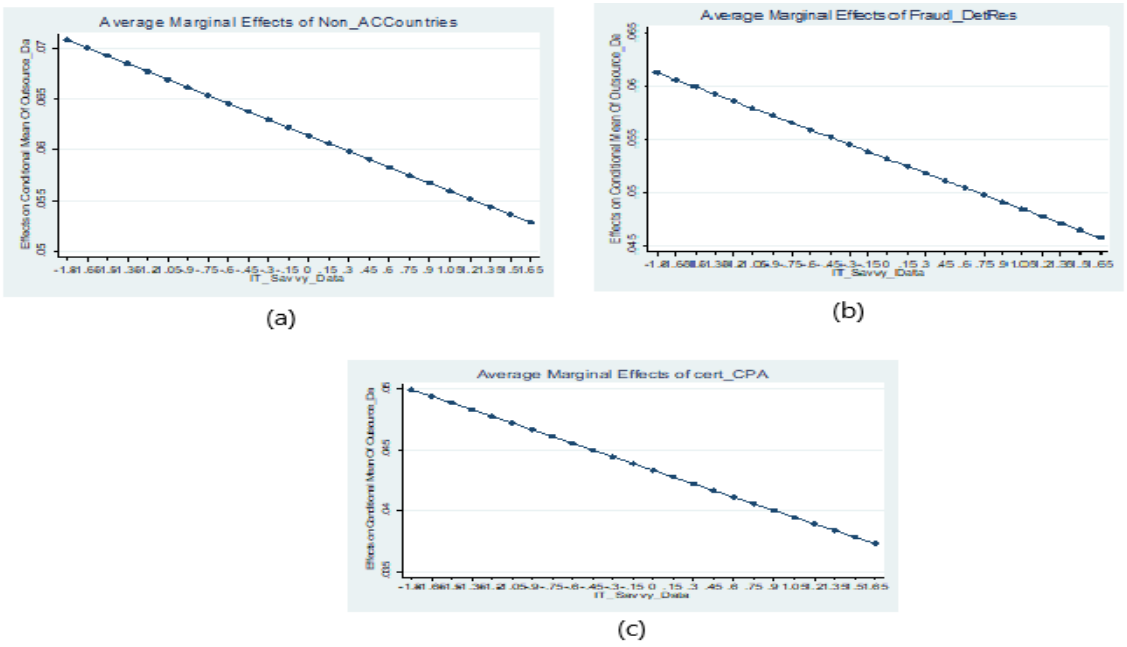


Figure 4.1 *Two-Way Interaction Effects*

Figure 4.2 shows the three-way interactions of significant variables. Figure 4.2(a) suggests that IAFs with fraud detection responsibilities in developing nations are most likely to outsource when they are low in data analytics skills. Overall, Figure 4.2(a) indicates that IAFs in developing nations are more likely to outsource and this likelihood increases further when they are assigned fraud detection responsibilities. The same finding also holds for other interactions variables. Taken together, the results suggest that

when IAFs are led by CPAs, or when IAFs are in developing nations, or when IAFs have fraud responsibilities, they are more likely to outsource analytics than other IAFs.

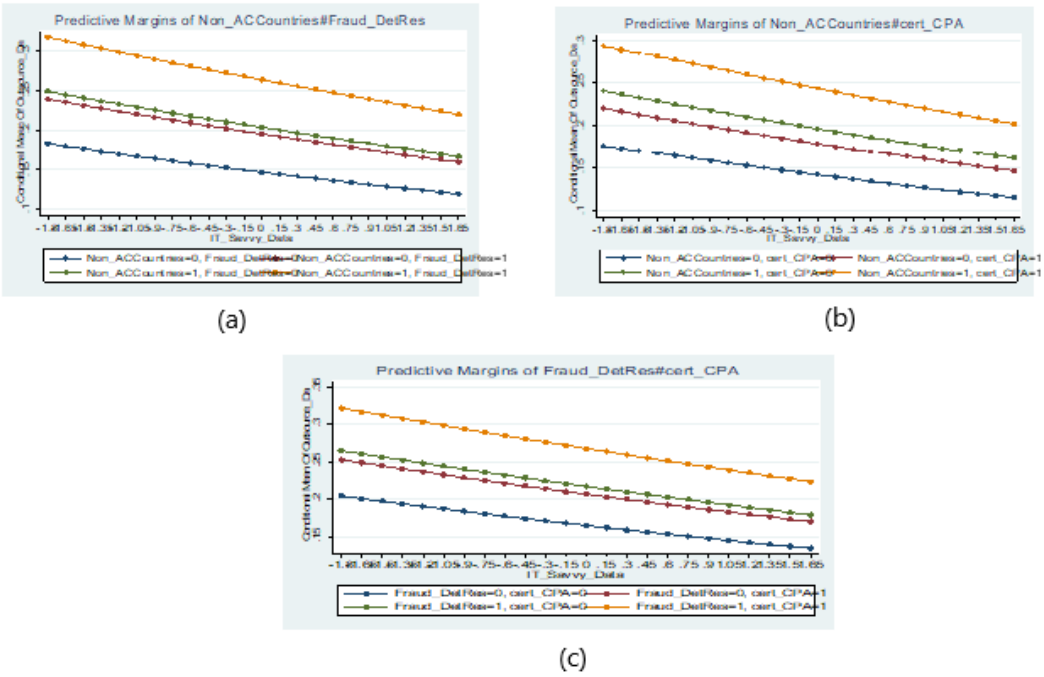


Figure 4.2 *Three-Way Interaction Effects*

Discussion and Conclusion

This study examines the determinants of outsourcing big data analytics by the Internal Audit Function (IAF). The importance of the study is reflected by the potential of data analytics to change the work processes of auditors. Though the information systems literature is rich in detail on the outsourcing topic, there is little outsourcing research in accounting. The study of the outsourcing of data analytics is important because the same individuals (IAFs) who provide data for outsourcing data analytics will also be directly affected by the outcome of those decisions and must rely on the work performed by the service organizations. Additionally, the complexity of this particular technology (i.e., data analytics) demands additional investigation of the sociologic, strategic, and

economic factors that determine the decision. Outsourced accounting functions must be performed in compliance with regulatory requirements, they are subject to external monitoring by regulatory authorities, and may they result in sanctions and significant penalties for non-compliance; thus, the outsourcing of big data analytics by IAFs warrants further investigation.

Drawing upon the Information System (IS) literature, the study hypothesizes that economic, strategic, and sociological factors play role in the IAFs' decision to outsource big data analytics. The results of the study suggest, contrary to conventional wisdom, that economic factors (as represented by the sufficiency of the budget allocated to IAFs) are not significant. Rather, strategic and sociological factors are significant in the outsourcing of big data analytics. Specifically, IAFs outsource big data analytics when they lack data skills and are tasked with fraud risk management. Additionally, the role of Chief Audit Executives (CAEs) is also significant. There is also a cultural variation in the outsourcing decision; IAFs from developing nations are more likely to outsource than are IAFs from developed countries. Further analysis of the interaction effects of these significant variables suggests that as the data skills of IAFs increase, the conditional difference of the likelihood of outsourcing decreases, suggesting that IAFs recognize both the value of data analytics and their lack of competencies. The three-way interactions of the variables support the same conclusion.

This study contributes to the literature in several ways. First, since outsourcing involves risks and because appropriate controls are required to mitigate those risks, insights into organizational motivations for outsourcing of analytics can help in identifying the appropriate control practices for developing outsourcing relationships.

Second, contrary to previous expectations that companies are more likely to outsource services that are common and rarely changed, the study provides evidence that this conventional wisdom does not apply for all situations, particularly as regards the outsourcing of accounting functions such as audit analytics. Third, the findings also inform external auditors who may be considering the evaluation of the objectivity and competence of IAFs before relying on their work. Finally, the findings add to our understanding about the role of accountants in outsourcing, in answer to the calls for research into the role of accountants and auditors in IT outsourcing processes.

There are limitations to the study. As in any survey research, data representing the responses of CAEs might not represent their real opinions, or may represent them unreliably, thus limiting the generality of results. Additionally, for data skills, there is no established scale and thus the construct might suffer from construct validity and reliability issues.

The research does provide opportunities for future research. For example, researchers can seek to understand the implications of the lack of data analytics skills on the part of IAFs, assessing whether it is due to the lack of necessary resources or if it is because they do not consider data analytics skills integral to the auditing function. Future research can also focus on how IAFs deal with the risks that arise from the decision to outsource data analytics.

CHAPTER 5

DISCUSSION AND CONCLUSION

This chapter summarizes the findings of three studies of the dissertation. Limitations of the studies are also described. Finally, the chapter concludes with directions for future research.

Study 1: Reaction of the Investors of Rivals Firms to the Information Security Breaches of Focal Firms: Evidence from Market Activity and Information Asymmetry

The study finds evidence that markets of rival firms react when focal firms experience data breaches. Particularly, the study documents that when focal firms announce data breaches, rival firms' trading volume and information asymmetry increases. However, the overall effects of data breaches to rival firms are opposite to those of focal firms; in many cases, rival firms' markets also react negatively. Specifically, I find that the characteristics of data breach types and previous data breach histories of focal firms have implications for rivals. However, strong information technology governance of rivals plays a shielding role in mitigating those negative effects. Further, though I hypothesized that strategic similarity of focals with rivals also has implications, the study did not document such effect. The results of the study are robust to alternative specifications of models and samples.

Study 2: Big Data Analytics Challenges and Internal Audit Function (IAF)'s Reliance on Big Data Analytics

Though big data analytics has potential to create value for accountants/auditors, data analytics are underutilized in the audit practice. The study examines the adoption of big data analytics by the Internal Audit Function (IAF) in view of several key challenges to adoption. The results of the study suggest that data-specific IT knowledge rather than general IT knowledge is significant in explaining the adoption of big data analytics. Critical thinking skills and business knowledge also contribute to the adoption of big data analytics.

If IAFs face challenges (management challenges) such as fraud risk detection, they are more likely to adopt big data analytics. Results from interaction effects analysis suggest that Chief Audit Executives (CAEs) with CPA certifications are more likely to adopt big data analytics than CAEs without CPA certifications, when the size of the organization is small, or when the size of the IAF is small, or when there is a lack of data-specific IT knowledge or business skills. Another important finding is that, when two groups of IAFs have similar size and data-specific IT knowledge, IAFs with fraud detection responsibility (management challenges) are more likely to adopt big data analytics. Finally, IAFs in Anglo culture countries are more likely to adopt big data analytics than IAFs in non-Anglo culture countries given that both IAFs have the same size and have data-specific IT knowledge. The study has both theoretical and practical implications, which are elaborated in the discussion of the contribution.

Study 3: Outsourcing of Big Data Analytics by Internal Audit Function

Big data analytics has the potential to fundamentally change the work process of auditors. The research studies the motivations of the Internal Audit Function (IAF) to outsource analytics. The results of the study suggest that, contrary to conventional wisdom, economic factors (as represented by the sufficiency of the budget allocated to IAFs) are not significant. Rather, strategic and sociological factors are significant in determining the outsourcing of big data analytics. Specifically, IAFs outsource big data analytics when they lack data skills and are tasked with fraud risk management responsibilities. Additionally, the role Chief Audit Executives (CAEs) is also significant. There is also a cultural variation in outsourcing decisions; IAFs from developing nations are more likely to outsource than are IAFs from developed countries. Further analysis of the interaction effects of these significant variables suggests that as the data skills of IAFs increase, the conditional difference of the likelihood of outsourcing decreases, suggesting that IAFs recognize both the value of data analytics and their specific lack of competencies in making such decisions. The three-way interactions of the variables support the same conclusion. The findings have implications about the formation of effective internal controls that will remediate risks arising from the outsourcing decision process. Moreover, external auditors will find the results useful when they evaluate the competence and objectivity of IAFs in determining whether to rely on their work.

Dissertation Limitations

The first study is subject to several limitations. Privacyrights.org does not cover the entire population of data breaches, therefore the analyzed sample is small.

Additionally, since the disclosure of data breaches is not required by the US Securities and Exchange Commission (SEC), there is wider latitude on the part of management on whether to disclose breaches.

As with all empirical survey investigations, the second study also bears limitations. The items used to measure latent constructs might not fully represent the construct because there are no established scales for the items related to data analytics in the literature. Moreover, for dependent variables, a few but highly representative areas, in which internal auditors can apply big data analytics were covered. There might be other inhibitors associated with incorporating big data into accounting that the study could not subsequently account for.

The third study is also subject to limitations. As is the case with all survey research, the responses here of CAEs might not represent their actual opinions, or may represent them inexactly, thus limiting generalization of the results. As in other studies of this dissertation, constructs are assessed for which prior scales did not exist, and subsequent issues of construct validity and reliability should always be taken into consideration when evaluating results.

Conclusion and Directions for Future Research

The findings of the dissertation can provide fruitful avenues for future research. Future studies should look for the other characteristics of data breaches or investigate other sorts of data breached firms, in order to discern further implications of breaches for rival firms. Most of the previous research that focus on a particular industry to examine the spillover effect of information security breaches used CAR for market reaction; one could also use abnormal turnover and abnormal bid-ask spread to examine market

reactions. Additionally, the effects of breaches on firms related to but not in competition with breached firms (e.g., suppliers or distributors in value chains) might well be studied in future research.

For the adoption of big data analytics by the IAF, future studies might focus on other issues such as security risk management of data which might have implications for the adoption of analytics. The role of CAEs with IT certification might also be explored, since their role was not significant in influencing the adoption of big data analytics. The third study of the dissertation also suggests future research opportunities. For example, researchers can seek to understand the reasons for the lack of data analytics skills on the part of IAFs – attempting to determine if it is because they lack necessary resources or because they do not consider data analytics skills as integral to the auditing function. Further, future research can focus on how IAFs deal with risks that arise from the decisions involved in outsourcing data analytics.

REFERENCES

Abbott, Lawrence J., Susan Parker, and Gary F. Peters. 2004. Audit committee characteristics and restatements. *Auditing: A Journal of Practice & Theory* 23 (1): 69–87.

Abdolmohammadi, Mohammad J., and Scott R. Boss. 2010. Factors associated with IT audits by the internal audit function. *International Journal of Accounting Information Systems* 11 (3): 140–151.

Abdolmohammadi, Mohammad J., Steven M. DeSimone, Tien-Shih Hsieh, and Zhihong Wang. 2017. Factors associated with internal audit function involvement with XBRL implementation in public companies: An international study. *International Journal of Accounting Information Systems* 25: 45–56.

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. 2006. Is there a cost to privacy breaches? An Event Study. *ICIS 2006 Proceedings*, 94.

Ahmi, Aidi, and Simon Kent. 2012. The utilisation of generalized audit software (GAS) by external auditors. *Managerial Auditing Journal* 28 (2): 88–113.

AICPA. 2015. Audit analytics and continuous audit: Looking toward the future. 2015. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/auditanalytics_lookingtowardfuture.pdf.

AICPA. 2017. Guide to audit data analytics fact sheet. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/guide-to-audit-data-analytics-fact-sheet-web.pdf.

Alles, Michael G. 2015. Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons* 29 (2): 439–449.

Alles, Michael, and Glen L. Gray. 2016. Incorporating big data in audits: Identifying inhibitors and a research agenda to address those inhibitors. *International Journal of Accounting Information Systems* 22: 44–59.

Amato, N. 2013. Three reasons finance should focus more on business intelligence. https://www.journalofaccountancy.com/news/2013/jul/20138385.html.

American Institute of Certified Public Accountants (AICPA). 2017. Description criteria for management's description of the entity's cybersecurity risk management program.

Anderson, Urton L., Margaret H. Christ, Karla M. Johnstone, and Larry E. Rittenberg. 2012. A post-SOX examination of factors associated with the size of internal audit functions. *Accounting Horizons* 26 (2): 167–191.

Andoh-Baidoo, Francis K., and Kweku-Muata Osei-Bryson. 2007. Exploring the characteristics of internet security breaches that impact the market value of breached firms. *Expert Systems with Applications* 32 (3): 703–725.

Appelbaum, Deniz. 2016. Securing big data provenance for auditors: The big data provenance black box as reliable evidence. *Journal of Emerging Technologies in Accounting* 13 (1): 17–36.

Apte, Uday M., Marion G. Sobol, Sho Hanaoka, Tatsumi Shimada, Timo Saarinen, Timo Salmela, and Ari PJ Vepsalainen. 1997. IS outsourcing practices in the USA, Japan and Finland: A comparative study. *Journal of Information Technology* 12 (4): 289–304.

Arthurs, J, S Cho, Y Choi, I Hemmatian, and A Joshi. 2015. The impact of bankruptcy on competitors: How technology knowledge overlap and diversification affect value redistribution. Working Paper. Oregon State University.

Bamber, Linda Smith. 1987. Unexpected earnings, firm size, and trading volume around quarterly earnings announcements. *Accounting Review* 62 (3): 510–532.

Bamber, Linda Smith, Orie E. Barron, and Douglas E. Stevens. 2011. Trading volume around earnings announcements and other financial reports: Theory, research design, empirical evidence, and directions for future research. *Contemporary Accounting Research* 28 (2): 431–471.

Bamber, Linda Smith, and Youngsoon Susan Cheon. 1995. Differential price and volume reactions to accounting earnings announcements. *Accounting Review*, 417–441.

Barnett, Michael L., and Andrew A. King. 2008. Good fences make good neighbors: A longitudinal analysis of an industry self-regulatory institution. *Academy of Management Journal* 51 (6): 1150–1170.

Barr-Pulliam, Dereck, Helen Brown-Liburd, and Kerri-Ann Sanderson. 2017. The effects of the internal control opinion and use of audit data analytics on perceptions of audit quality, assurance, and auditor negligence. *Working Paper, University of Wisconsin - Madison*.

Barton, Dominic, and D. Court. 2012. Making advanced analytics work for you. *Harvard Business Review* 90 (10): 78–83.

Baysinger, Barry, and Robert E. Hoskisson. 1989. Diversification strategy and r&d intensity in multiproduct firms. *Academy of Management Journal* 32 (2): 310–332.

Beasley, Mark S., Joseph V. Carcello, and Dana R. Hermanson. 1999. Fraudulent financial reporting: 1987-1997, an analysis of US public companies. *The Auditors' Report* 22 (3): 15–17.

Beaver, William H. 1968. The information content of annual earnings announcements. *Journal of Accounting Research*, 67–92.

Bierstaker, James, Diane Janvrin, and D. Jordan Lowe. 2014. What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting* 30 (1): 67–74.

Blaskovich, Jennifer, and Natalia Mintchik. 2011. Information technology outsourcing: A taxonomy of prior studies and directions for future research. *Journal of Information Systems* 25 (1): 1–36.

Blue Ribbon Committee. 1999. Report and recommendations of the blue ribbon committee on improving the effectiveness of corporate audit committees. *The Business Lawyer*, 1067–1095.

Bollen, Johan, Huina Mao, and Xiaojun Zeng. 2011. Twitter mood predicts the stock market. *Journal of Computational Science* 2 (1): 1–8.

Braun, Robert L., and Harold E. Davis. 2003. Computer-assisted audit tools and techniques: Analysis and perspectives. *Managerial Auditing Journal* 18 (9): 725–731.

Brown-Liburd, Helen, Hussein Issa, and Danielle Lombardi. 2015. Behavioral implications of big data's impact on audit judgment and decision-making and future research directions. *Accounting Horizons* 29 (2): 451–468.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11 (3): 431–448.

Cao, Min, Roman Chychyla, and Trevor Stewart. 2015. Big data analytics in financial statement audits. *Accounting Horizons* 29 (2): 423–429.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9 (1): 70–104.

CBOK. 2015. Common body of knowledge in internal auditing. The Institute of Internal Auditors Research Foundation.

Chan, Konan, Li Ge, and Tse-Chun Lin. 2015. Informational content of options trading on acquirer announcement return. *Journal of Financial and Quantitative Analysis* 50 (5): 1057–1082.

Chen, Lucy Huajing, Saiying Deng, Parveen P. Gupta, and Heibatollah Sami. 2015. The SEC's elimination of 20-f reconciliation and information asymmetry. *Journal of Contemporary Accounting & Economics* 11 (1): 75–87.

Chen, Lucy Huajing, and Heibatollah Sami. 2008. Trading volume reaction to the earnings reconciliation from IAS to US GAAP. *Contemporary Accounting Research* 25 (1): 15–53.

Chen, Lucy Huajing, and Heibatollah Sami. 2013. The impact of firm characteristics on trading volume reaction to the earnings reconciliation from IFRS to US GAAP. *Contemporary Accounting Research* 30 (2): 697–718.

Cho, Seong Y., Cheol Lee, and Ray J. Pfeiffer Jr. 2013. Corporate social responsibility performance and information asymmetry. *Journal of Accounting and Public Policy* 32 (1): 71–83.

Christ, Margaret H., Adi Masli, Nathan Y. Sharp, and David A. Wood. 2015. Rotational internal audit programs and financial reporting quality: Do compensating controls help? *Accounting, Organizations and Society* 44: 37–59.

Christ, Margaret H., Natalia Mintchik, Long Chen, and James L. Bierstaker. 2015. Outsourcing the information system: Determinants, risks, and implications for management control systems. *Journal of Management Accounting Research* 27 (2): 77–120.

Coller, Maribeth, and Teri Lombardi Yohn. 1997. Management forecasts and information asymmetry: An examination of bid-ask spreads. *Journal of Accounting Research* 35 (2): 181–191.

Collins, Daniel W., Jaewoo Kim, and Heejin Ohn. 2018. Do mandatory accounting disclosures impair disclosing firms' competitiveness? Evidence from mergers and acquisitions. *Working Paper, University of Iowa, University of Rochester*.

Columbus, Louis. 2017. 53% of companies are adopting big data analytics. *Forbes*, 2017. https://www.forbes.com/sites/louiscolumbus/2017/12/24/53-of-companies-are-adopting-big-data-analytics/.

Connelly, Brian L., S. Trevis Certo, R. Duane Ireland, and Christopher R. Reutzel. 2011. Signaling theory: A review and assessment. *Journal of Management* 37 (1): 39–67.

Corwin, Shane A., and Paul Schultz. 2012. A simple way to estimate bid-ask spreads from daily high and low prices. *The Journal of Finance* 67 (2): 719–760.

Crawley, Michael, and James Wahlen. 2014. Analytics in empirical/archival financial accounting research. *Business Horizons* 57 (5): 583–593.

Cready, William M., and David N. Hurtt. 2002. Assessing investor response to information events using return and volume metrics. *The Accounting Review* 77 (4): 891–909.

Cready, William M., and Patricia G. Mynatt. 1991. The information content of annual reports: A price and trading response analysis. *Accounting Review*, 291–312.

Curtis, Mary B., and Elizabeth A. Payne. 2008. An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems* 9 (2): 104–121.

Dai, Jun, and Miklos A. Vasarhelyi. 2016. Imagineering audit 4.0. *Journal of Emerging Technologies in Accounting* 13 (1): 1–15.

Davis, Angela K., Jeremy M. Piger, and Lisa M. Sedor. 2012. Beyond the numbers: Measuring the information content of earnings press release language. *Contemporary Accounting Research* 29 (3): 845–868.

Debreceny, Roger, Sook-Leng Lee, Willy Neo, and Jocelyn Shuling Toh. 2005. Employing generalized audit software in the financial services sector: Challenges and opportunities. *Managerial Auditing Journal* 20 (6): 605–618.

Deloitte. 2016a. Deloitte form aliance with kira systems. 2016. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-forms-alliance-with-kira-systems-to-drive-the-adoption-of-artificial-intelligence-in-the-workplace.html.

Deloitte. 2016b. Internal Audit Analytics: The journey to 2020. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-internalaudit- analytics-pov.pdf.

Dorta, M. 2016. Introduction to fractional outcome regression models using the Fracreg and Betareg commands. STATA. https://www.stata.com/meeting/mexico16/slides/Mexico16_Dorta.pdf.

Earley, Christine E. 2015. Data analytics in auditing: Opportunities and challenges. *Business Horizons* 58 (5): 493–500.

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. 2016. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity* 2 (1): 3–14.

Egginton, Jared F., and William R. McCumber. 2018. Executive network centrality and stock liquidity. *Financial Management*.

Erhardt, K. 2016. Training the auditor of 2020. *Internal Auditor* 73 (1): 69.

Ettredge, Michael L., and Vernon J. Richardson. 2003. Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71–82.

EY. 2014. Big risks require big data thinking. 2014. http://www.ey.com/Publication/vwLUAssets/EY-Global-Forensic-Data-Analytics-Survey-2014/$FILE/EY-Global-Forensic-Data-Analytics-Survey-2014.pdf.

EY. 2015. How big data and analytics are transforming the audit. 2015. http://www.ey.com/gl/en/services/assurance/ey-reporting-issue-9-how-big-data-and-analytics-are-transforming-the-audit.

Fama, E. 1970. The behavior of stock market prices. *The Journal of Finance* 25: 383–417.

Farah, Nusrat. 2017. Impact of mergers & acquisition on rivals: The role of competitive dynamics in mergers & acquisitions. Working Paper. Oregon State University.

Feldman, Ronen, Suresh Govindaraj, Joshua Livnat, and Benjamin Segal. 2010. Management's tone change, post earnings announcement drift and accruals. *Review of Accounting Studies* 15 (4): 915–953.

Feng, Cecilia Qian, and Tawei Wang. 2018. Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*.

Ferris, Stephen P., Narayanan Jayaraman, and Anil K. Makhija. 1997. The response of competitors to announcements of bankruptcy: An empirical examination of contagion and competitive effects. *Journal of Corporate Finance* 3 (4): 367–395.

Foucault, Thierry, and Laurent Fresard. 2014. Learning from peers' stock prices and corporate investment. *Journal of Financial Economics* 111 (3): 554–577.

Franz, Diana R., Ramesh P. Rao, and Niranjan Tripathy. 1995. Informed trading risk and bid-ask spread changes around open market stock repurchases in the nasdaq market. *Journal of Financial Research* 18 (3): 311–327.

Frino, Alex, Stewart Jones, and Jin Boon Wong. 2007. Market behaviour around bankruptcy announcements: Evidence from the australian stock exchange. *Accounting & Finance* 47 (4): 713–730.

Fullerton, Laurie. 2016. "KPMG Collaborates with IBM Watson to Usher in Era of Cognitive Computing." 2016. http://www.thedrum.com/news/2016/03/08/kpmg-collaborates-ibm-watson-usher-era-cognitive-computing.

Gatzlaff, Kevin M., and Kathleen A. McCullough. 2010. The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review* 13 (1): 61–83.

Gillette, Ann B., Douglas E. Stevens, Susan G. Watts, and Arlington W. Williams. 1999. Price and volume reactions to public information releases: An experimental approach incorporating traders' subjective beliefs. *Contemporary Accounting Research* 16 (3): 437–479.

Gimeno, Javier, and Carolyn Woo. 1996. Hypercompetition in a multimarket environment: The role of strategic similarity and multimarket contact in competitive de-escalation. *Organization Science* 7 (3): 322–41.

Gleason, Cristi A., Nicole Thorne Jenkins, and W. Bruce Johnson. 2008. The contagion effects of accounting restatements. *The Accounting Review* 83 (1): 83–110.

Gonzalez, George C., Pratyush N. Sharma, and Dennis F. Galletta. 2012. The antecedents of the use of continuous auditing in the internal auditing context. *International Journal of Accounting Information Systems* 13 (3): 248–262.

Haensly, Paul J., John Theis, and Zane Swanson. 2001. Reassessment of contagion and competitive intra-industry effects of bankruptcy announcements. *Quarterly Journal of Business and Economics*, 45–63.

Hagigi, Moshe, Brian D. Kluger, and David Shields. 1993. Auditor change announcements and dispersion of investor expectations. *Journal of Business Finance & Accounting* 20 (6): 787–802.

Hair, J., R. Anderson, R. Tatham, and W. Black. 1998. *Multivariate data analysis*. 5th ed. NJ: Upper Saddle River, NJ: Prentice Hall.

Haislip, Jacob, Jee-Hae Lim, and Rob Pinsker. 2017. Do the roles of the ceo and cfo differ when it comes to data security breaches? In *Twenty-Third Americas Conference on Information Systems*. Boston, MA.

Haislip, Jacob, A. Masli, V.J. Richardson, and J.M. Sanchez. 2016. Repairing organizational legitimacy following information technology (it) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. *Journal of Information Systems* 30 (1): 41–70.

Haislip, Jacob, Adi Masli, Vernon J. Richardson, and Watson Marcia. 2015. External reputational penalties for ceos and cfos following information technology material weaknesses. *International Journal of Accounting Information Systems* 17: 1–15.

Hall, James A. 2005. Financial performance, ceo compensation, and large-scale information technology outsourcing decisions. *Journal of Management Information Systems* 22 (1): 193–221.

HBGary Inc. 2013. Cybersecurity directly affects investor attitudes, new HBGary survey finds. 2013. https://www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html.

Héroux, Sylvie, and Anne Fortin. 2013. The internal audit function in information technology governance: A holistic perspective. *Journal of Information Systems* 27 (1): 189–217.

Higgs, Julia L., Robert E. Pinsker, Thomas J. Smith, and George R. Young. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30 (3): 79–98.

Hinz, Oliver, Michael Nofer, Dirk Schiereck, and Julian Trillig. 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management* 52 (3): 337–347.

Hoberg, Gerard, and Gordon Phillips. 2010. Product market synergies and competition in mergers and acquisitions: A text-based analysis. *The Review of Financial Studies* 23 (10): 3773–3811.

Hoberg, Gerard, and Gordon Phillips. 2016. Text-based network industries and endogenous product differentiation. *Journal of Political Economy* 124 (5): 1423–1465.

Holt, Matthew, Bradley Lang, and Steve G. Sutton. 2017. Potential employees' ethical perceptions of active monitoring: The dark side of data analytics. *Journal of Information Systems* 31 (2): 107–124.

Hovav, Anat, and John D'Arcy. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6 (2): 97–121.

Hovav, Anat, and John D'Arcy. 2004. The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13 (3): 32–40.

Huerta, Esperanza, and Scott Jensen. 2017. An accounting information systems perspective on data analytics and big data. *Journal of Information Systems* 31 (3): 101–114.

IIA. 2016. International standards for the professional practice of internal auditing. 2016. https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf.

International Data Corporation. 2015. Worldwide semiannual big data and analytics spending guide. IDC: The premier global market intelligence company. 2015. https://www.idc.com/getdoc.jsp?containerId=IDC_P33195.

Islam, Md Shariful, Nusrat Farah, and Thomas F. Stafford. 2018. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal* 33 (4): 377–409.

Janvrin, Diane, James Bierstaker, and D. Jordan Lowe. 2008. An examination of audit information technology use and perceived importance. *Accounting Horizons* 22 (1): 1–21.

Janvrin, Diane, James Bierstaker, and D. Jordan Lowe. 2009. An investigation of factors influencing the use of computer-related audit procedures. *Journal of Information Systems* 23 (1): 97–118.

Jeong, Christina Y., Sang-Yong Tom Lee, and Jee-Hae Lim. 2018. Information security breaches and it security investments: Impacts on competitors. *Information & Management*.

Josefy, Matthew, Scott Kuban, R. Duane Ireland, and Michael A. Hitt. 2015. All things great and small: Organizational size, boundaries of the firm, and a changing environment. *The Academy of Management Annals* 9 (1): 715–802.

Juniper Research. 2015. Cybercrime will cost businesses over $2 trillion by 2019. 2015. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

Kannan, Karthik, Jackie Rees, and Sanjay Sridhar. 2007. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12 (1): 69–91.

Kashmiri, Saim, Cameron Duncan Nicol, and Liwu Hsu. 2017. Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of IT, Marketing, and CSR. *Journal of the Academy of Marketing Science* 45 (2): 208–228.

Katz, D. 2014. Regulators fear big data threatens audit quality. http://ww2.cfo.com/auditing/2014/04/regulators-fear-big-data-threatens-audit-quality/.

Kim, Hyo-Jeong, Michael Mannino, and Robert J. Nieschwietz. 2009. Information technology acceptance in the internal audit profession: Impact of technology features and complexity. *International Journal of Accounting Information Systems* 10 (4): 214–228.

Kim, Oliver, and Robert E. Verrecchia. 1991. Trading volume and price reactions to public announcements. *Journal of Accounting Research*, 302–321.

Kothari, Sabino P., Xu Li, and James E. Short. 2009. The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review* 84 (5): 1639–1670.

KPMG. 2015. 2015 Survey - Data and analytics enabled internal audit. 2015. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/DA-Enabled-Internal-Audit-Survey.pdf.

Krahel, John Peter, and William R. Titera. 2015. Consequences of big data and formalization on accounting and auditing standards. *Accounting Horizons* 29 (2): 409–422.

Kwon, Juhee, Jackie Rees Ulmer, and Tawei Wang. 2012. The association between top management involvement and compensation and information security breaches. *Journal of Information Systems* 27 (1): 219–236.

Lang, Larry HP, and RenéM Stulz. 1992. Contagion and competitive intra-industry effects of bankruptcy announcements: An empirical analysis. *Journal of Financial Economics* 32 (1): 45–60.

Lehavy, Reuven, Feng Li, and Kenneth Merkley. 2011. The effect of annual report readability on analyst following and the properties of their earnings forecasts. *The Accounting Review* 86 (3): 1087–1115.

Lepak, David P., Riki Takeuchi, and Scott A. Snell. 2003. Employment flexibility and firm performance: Examining the interaction effects of employment mode, environmental dynamism, and technological intensity. *Journal of Management* 29 (5): 681–703.

Li, Feng. 2008. Annual report readability, current earnings, and earnings persistence. *Journal of Accounting and Economics* 45 (2–3): 221–247.

Li, Feng. 2010a. Managers' self-serving attribution bias, overconfidence, and corporate financial policies. University of Michigan working paper.

Li, Feng. 2010b. Textual analysis of corporate disclosures: A survey of the literature. *Journal of Accounting Literature* 29: 143.

Li, Feng. 2010c. The information content of forward-looking statements in corporate filings—a naïve bayesian machine learning approach. *Journal of Accounting Research* 48 (5): 1049–1102.

Li, Feng, Russell Lundholm, and Michael Minnis. 2013. A measure of competition based on 10-k filings. *Journal of Accounting Research* 51 (2): 399–436.

Li, He, Jun Dai, Tatiana Gershberg, and Miklos A. Vasarhelyi. 2018. Understanding usage and value of audit analytics for internal auditors: An organizational approach. *International Journal of Accounting Information Systems* 28: 59–76.

Liu, W, and J Xin. 2014. Modeling fractional outcomes with SAS ®. SAS. http://support.sas.com/resources/papers/proceedings14/1304-2014.pdf.

Loughran, Tim, and Bill McDonald. 2010. Measuring readability in financial text. Working Paper. The University of Notre Dame.

Mahzan, Nurmazilah, and Andy Lymer. 2014. Examining the adoption of computer-assisted audit tools and techniques: Cases of generalized audit software use by internal auditors. *Managerial Auditing Journal* 29 (4): 327–349.

Malaescu, Irina, and Steve G. Sutton. 2015. The reliance of external auditors on internal audit's use of continuous audit. *Journal of Information Systems* 29 (1): 95–114.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81 (1): 36–58.

Miller, Brian P. 2010. The effects of reporting complexity on small and large investor trading. *The Accounting Review* 85 (6): 2107–2143.

Murphy, M., and K. Tysiac. 2015. Data analytics helps auditors gain deep insight. https://www.journalofaccountancy.com/issues/2015/apr/data-analytics-for-auditors.html.

Nelson, Karen K., and Adam C. Pritchard. 2007. Litigation risk and voluntary disclosure: The use of meaningful cautionary language. In *2nd Annual Conference on Empirical Legal Studies Paper*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998590.

Osborn, Richard N., and C. Christopher Baughn. 1990. Forms of interorganizational governance for multinational alliances *Academy of Management Journal* 33 (3): 503–519.

Paruchuri, Srikanth, and Vilmos F. Misangyi. 2015. Investor perceptions of financial misconduct: The heterogeneous contamination of bystander firms. *Academy of Management Journal* 58 (1): 169–194.

PCAOB. 2007. AS 2201: An audit of internal control over financial reporting that is integrated with an audit of financial statements. 2007. https://pcaobus.org:443/Standards/Auditing/Pages/AS2201.aspx.

PCAOB. 2012. AS 1301: Communications with audit committees. 2012. https://pcaobus.org:443/Standards/Auditing/Pages/AS1301.aspx.

Pennington, Robin R., Andrea S. Kelton, and Delwyn D. DeVries. 2006. The effects of qualitative overload on technology acceptance. *Journal of Information Systems* 20 (2): 25–36.

Ponemon Institute. 2017. 2017 Cost of cybercrime study. 2017. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017.

Premuroso, Ronald F., and Somnath Bhattacharya. 2007. Is there a relationship between firm performance, corporate governance, and a firm's decision to form a technology committee? *Corporate Governance: An International Review* 15 (6): 1260–1276.

Protiviti. 2017. Embracing analytics in auditing. 2017. https://www.protiviti.com/sites/default/files/united_states/insights/2017-internal-auditcapabilities- and-needs-survey-protiviti.pdf.

Provost, Foster, and Tom Fawcett. 2013. Data science and its relationship to big data and data-driven decision-making. *Big Data* 1 (1): 51–59.

PwC. 2015. Data driven: What students need to succeed in a rapidly changing business world. 2015. https://cpb-us-west-2-juc1ugur1qwqqqo4.stackpathdns.com/sites.gsu.edu/dist/1/1670/files/2015/08/pwc-data-driven-paper-1wdb00u.pdf.

Richins, Greg, Andrea Stapleton, Theophanis C. Stratopoulos, and Christopher Wong. 2017. Big data analytics: Opportunity or threat for the accounting profession? *Journal of Information Systems* 31 (3): 63–79.

Rogers, Jonathan L., and Andrew Van Buskirk. 2009. Shareholder litigation and changes in disclosure behavior. *Journal of Accounting and Economics* 47 (1–2): 136–156.

Rosati, Pierangelo, Mark Cummins, Peter Deeney, Fabian Gogolin, Lisa van der Werff, and Theo Lynn. 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis* 49: 146–154.

Rose, Anna M., Jacob M. Rose, and Carolyn S. Norman. 2013. Is the objectivity of internal audit compromised when the internal audit function is a management training ground? *Accounting & Finance* 53 (4): 1001–1019.

Rose, Anna M., Jacob M. Rose, Kerri-Ann Sanderson, and Jay C. Thibodeau. 2017. When should audit firms introduce analyses of big data into the audit process? *Journal of Information Systems* 31 (3): 81–99.

Schneider, Gary P., Jun Dai, Diane J. Janvrin, Kemi Ajayi, and Robyn L. Raschke. 2015. Infer, predict, and assure: Accounting opportunities in data analytics. *Accounting Horizons* 29 (3): 719–742.

Securities and Exchange Commission (SEC). 2011. CF disclosure guidance: topic no. 2 - cybersecurity. 2011. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Sheikh, Shahbaz. 2018. The impact of market competition on the relation between ceo power and firm innovation. *Journal of Multinational Financial Management* 44: 36–50.

Simmonds, Kenneth. 1982. Strategic management accounting for pricing: A case example. *Accounting and Business Research* 12 (47): 206–214.

Sivarajah, Uthayasankar, Muhammad Mustafa Kamal, Zahir Irani, and Vishanth Weerakkody. 2017. Critical analysis of big data challenges and analytical methods. *Journal of Business Research* 70: 263–286.

Smith, Michael Alan, Sabyasachi Mitra, and Sridhar Narasimhan. 1998. Information systems outsourcing: A study of pre-event firm characteristics. *Journal of Management Information Systems* 15 (2): 61–93.

Sobol, Marion G., and Uday Apte. 1995. Domestic and global outsourcing practices of america's most effective IS users. *Journal of Information Technology* 10 (4): 269–280.

Tang, Fengchun, Carolyn Strand Norman, and Valaria P. Vendrzyk. 2017. Exploring perceptions of data analytics in the internal audit function. *Behaviour & Information Technology* 36 (11): 1125–1136.

The Economist. 2017. The world's most valuable resource is no longer oil, but data, May 6, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data?fsrc=scn/tw/te/rfd/pe.

Turel, Ofir, and Chris Bart. 2014. Board-level IT governance and organizational performance. *European Journal of Information Systems* 23 (2): 223–239.

Turel, Ofir, Peng Liu, and Chris Bart. 2017. Board-level information technology governance effects on organizational performance: The roles of strategic alignment and authoritarian governance. *Information Systems Management* 34 (2): 117–36.

Uhlenbruck, Klaus, Margaret Hughes-Morgan, Michael A. Hitt, Walter J. Ferrier, and Rhett Brymer. 2017. Rivals' reactions to mergers and acquisitions. *Strategic Organization* 15 (1): 40–66.

Vasarhelyi, Miklos A., Alexander Kogan, and Brad M. Tuttle. 2015. Big data in accounting: An overview. *Accounting Horizons* 29 (2): 381–396.

Verver, J. 2015. Six audit analytics success factors. *Internal Auditor* 72 (3): 20–21.

Walters, Riley. 2015. Cyber-attacks on U.S. companies since November 2014. The Heritage Foundation. 2015. /cybersecurity/report/cyber-attacks-us-companies-november-2014.

Wamba, Samuel Fosso, Angappa Gunasekaran, Shahriar Akter, Steven Ji-fan Ren, Rameshwar Dubey, and Stephen J. Childe. 2017. Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research* 70: 356–365.

Wang, Tawei, and Robert Cuthbertson. 2015. Eight issues on audit data analytics we would like researched. *Journal of Information Systems* 29 (1): 155–162.

Warren Jr, J. Donald, Kevin C. Moffitt, and Paul Byrnes. 2015. How big data will change accounting. *Accounting Horizons* 29 (2): 397–407.

Yayla, Ali Alper, and Qing Hu. 2011. The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology* 26 (1): 60–77.

Yoon, Kyunghee, Lucas Hoogduin, and Li Zhang. 2015. Big data as complementary audit evidence. *Accounting Horizons* 29 (2): 431–438.

Zafar, Humayun, Myung Ko, and Kweku-Muata Osei-Bryson. 2012. Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal (IRMJ)* 25 (1): 21–37.

Zafar, Humayun, Myung S. Ko, and Kweku-Muata Osei-Bryson. 2016. The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers* 18 (6): 1205–1215.

Zhang, Juan, Xiongsheng Yang, and Deniz Appelbaum. 2015. Toward effective big data analysis in continuous auditing. *Accounting Horizons* 29 (2): 469–476.

APPENDIX A

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT ("Agreement") is entered into on this <04-14-2017> ("Effective Date") by and between the Internal Audit Foundation (the Foundation), a not-for-profit incorporated in the Washington, D.C., ("the Foundation") and < Md. Shariful Islam > ("Contractor") (both hereinafter referred to as "Parties")

The Parties agree as follows:

1. **Disclosing Party**. For the purposes herein, the Disclosing Party is the Foundation where said party provides information to the Contractor.
2. **Receiving Party**. For the purposes herein, the Receiving Party is the Contractor where said party receives information from the Foundation.
3. **Purpose.** See Attachment A: Data Access Request Form. ("Purpose")
4. **Confidential Information.** For purposes herein, "Confidential Information" shall mean any and all information of a confidential nature that the Disclosing Party discloses to the Receiving Party, including, but not limited to specifications, formulas, prototypes, computer programs and any and all records, data, ideas, methods, techniques, processes and projections, plans, business plans, marketing information, materials, financial statements, memoranda, analyses, notes, legal documents and other data and information, regardless of form, as well as improvements, patents (whether pending or duly registered) and any know-how related thereto, as well as any information learned by the Receiving Party from the Disclosing Party through inspection of the Disclosing Party's property and/or its products and/or designs, and any third-party confidential information disclosed to the Receiving Party by the Disclosing Party.

Notwithstanding, Confidential Information shall not include information that: (i) is now or subsequently becomes generally available in the public domain through no fault or breach on the part of the Receiving Party; (ii) the Receiving Party can demonstrate in its records to have had rightfully in its possession prior to disclosure of the Confidential Information by the Disclosing Party; (iii) Receiving Party rightfully obtains from a third party who has the right to transfer or disclose it, without default or breach of confidentiality obligation; (iv) the Receiving Party can demonstrate in its records to have independently developed, without breach of this Agreement and/or any use or reference to the Disclosing Party's Confidential Information; or (v) is disclosed pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided, however, that the Receiving Party shall make the best effort to provide prompt notice of such court order or requirement to the Disclosing Party to enable the Disclosing Party to seek a protective order or otherwise prevent or restrict such disclosure.

For the purpose of the foregoing exceptions, disclosures which are specific, such as design practices and techniques, products, software, operating parameters, etc. shall not be deemed to be within the foregoing exceptions merely because they are embraced by general disclosures which are in the public domain or in the possession of the Receiving Party. In addition, any combination of features shall not be deemed to be within the foregoing exceptions merely because individual features thereof are in the public domain or in the possession of the Receiving Party, but only if the combination itself and its principle of operation are in the public domain or in the possession of the Receiving Party. Furthermore, certain

information may be generally known in the relevant industry, but the fact that the Disclosing Party uses it may not be so known, and therefore, such information shall be treated as Confidential Information.

5. **Non-disclosure and Non-use.** The Receiving Party agrees to accept and use Confidential Information solely for the Purpose. The Receiving Party will not disclose, publish, or disseminate Confidential Information to a third party. The Receiving Party further agrees to take all reasonable precautions to prevent any unauthorized use, disclosure, publication, or dissemination of Confidential Information to any third party. The Receiving Party agrees not to use Confidential Information otherwise for its own or any third party's benefit without the prior written approval of an authorized representative of the Disclosing Party in each instance. In performing its duties and obligations hereunder, the Receiving Party agrees to use at least the same degree of care as it does with respect to its own confidential information of like importance but, in any event, at least reasonable care. Further, the Receiving Party agrees that it shall not make any copies of the Confidential Information on any type of media, without the prior express written permission of the authorized representative of the Disclosing Party, other than for the fulfillment of the Purpose.
6. **Ownership.** All Confidential Information, and any derivatives thereof is and shall remain the property of the Disclosing Party and no license or other rights to Confidential Information is granted or implied hereby to have been granted to the Receiving Party, now or in the future.

7. **No Warranty.** The Confidential Information and any other information is provided by the disclosing party "as is", without any warranty, whether express or implied, as to its accuracy or completeness, operability, use, fitness for a particular purpose, or non-infringement.

8. **Return of Confidential Information.** Nothing herein shall be construed as imposing an obligation on the Disclosing Party to disclose, now or in the future, Confidential Information to the Receiving Party. The Disclosing Party may, at any time, with or without cause, demand the return of the Confidential Information, or any part thereof, by giving written notice to the Receiving Party, with immediate effect. Upon the earlier of: (i) the Disclosing Party's foregoing written notice or (ii) the termination, or expiration of this Agreement as set forth in paragraph eight below, the Receiving Party shall forthwith:

   (a) return to the Disclosing Party any information disclosed in any tangible form, and all copies thereof (on whatever physical, electronic or other media such information may be stored) containing any of the Confidential Information, unless such Confidential Information is stored in electronic form, in which case it is to be immediately deleted; and

   (b) provide a written certification that the Receiving Party has complied with all of the terms of this Agreement, that it has retained no copies of the Confidential Information on any media and that it has retained no notes, or other embodiments, of the Confidential Information.

9. **Equitable Relief.** The Receiving Party hereby acknowledges that unauthorized disclosure or use of Confidential Information may cause irreparable harm and

significant injury to the Disclosing Party that may be difficult to ascertain. Accordingly, the Receiving Party agrees that the Disclosing Party, without prejudice to any other right or remedy that it may have available to it at law or in equity, will have the right to seek and obtain immediate injunctive relief to enforce obligations under this Agreement without the necessity of proving actual damages and without the necessity of posting bond or making any undertaking in connection therewith.

10. **Entire Agreement and Governing Law.** The laws of the State of Florida govern all matters arising out of this Agreement. Any action to enforce any terms of this Agreement must be brought in Seminole County, Florida and both parties consent to a court of competent jurisdiction in that state.
11. **Term.** This Agreement shall govern the communications relating to Confidential Information between the Parties hereto as of the Effective Date, and shall expire or terminate upon the earlier of the following to occur: (i) the period of two (2) years; or (ii) until such time as the present Agreement is expressly superseded by a subsequent agreement between the Parties hereto; or, (iii) upon termination of the Agreement by either Party hereto, at any time, with or without cause, subject to a seven (7) day prior written notice (hereinafter, all of the above "Term"). The obligations set forth in this Agreement shall bind the Parties for a period of three (3) years from the date of disclosure of the Confidential Information or any part thereof, and such obligations shall survive the termination or earlier expiration of this Agreement.

12. **Assignment.** This Agreement shall not be assignable by either party without the prior written consent of the other party, and any purported assignment not permitted hereunder shall be construed null and void. However, it is hereby clarified that consent of the Receiving Party shall not be required for the terms and conditions of this agreement to apply towards the company formed by the Disclosing party upon its incorporation.

    The parties are signing this agreement on the Effective Date, which is stated in the introductory clause.

[INSERT]

Md. Shariful Islam

By: _____
Authorized Signature

Md. Shariful Islam
Name

Doctoral Student
Title

Louisiana Tech University
Organization

Sharif10.ais.du2004@gmail.com
Email Address

318 W Louisiana Avenue, Lot # 01, Ruston Louisiana 71270
Address

318 W Louisiana Avenue, Lot # 01, Ruston Louisiana 71270
Address

Louisiana Tech y
Institute Affiliation

Internal Audit Foundation

Bonnie Ulmer

By: _____
Authorized Signature

Bonnie Ulmer
Name

Vice President
Title