CAN YOU SEE IT COMING? HOW DISCLOSURE AND CORPORATE SOCIAL RESPONSIBILITY ACTIVITY PREDICT CYBERSECURITY BREACH

By

Marcy Ruthann Binkley

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Business Administration

Charlotte

2021

Approved by:

____
Dr. Laura Stanley

____
Dr. Marcia Watson

____
Dr. Gregory Martin

____
Dr. Chandra Subramaniam

ABSTRACT

MARCY RUTHANN BINKLEY. Can You See It Coming? How Disclosure and Corporate Social Responsibility Activity Predict Cybersecurity Breach. (Under the direction of DR. LAURA STANLEY)

This dissertation explores the cybersecurity risk disclosure and the information an organization signals via disclosure contents. Extant literature acknowledges the ability of the cybersecurity risk disclosure to predict subsequent related outcome (i.e., realization of breach incident). However, little research has addressed whether the disclosure signals important information about the IT Risk Culture governing the organization. To fill this gap, I examine cybersecurity risk disclosures using textual analysis and clustering techniques to analyze the IT Risk Culture of a sample of organizations between the years 2011 – 2019. Three classifications of IT Risk Culture are identified. I find that a certain IT Risk Culture, evidenced by the vulnerability and the propensity for risk transfer (i.e. cybersecurity insurance) expressed in the cybersecurity risk disclosure, is associated with subsequent cybersecurity breach. Additionally, the disclosure of Corporate Social Responsibility activity is found to be associated with a second classification of IT Risk Culture, one in which there is no significant association with subsequent cybersecurity breach. This dissertation contributes to holistic risk management literature by employing a systems perspective of IT Risk Culture to analyze related disclosures. Findings contribute greatly to the understanding of IT Risk Culture classification, predominant risk response behavior and the likelihood of subsequent related outcomes.

ACKNOWLEDGEMENTS

I would like to thank my husband, Brennon, and our two children, Bailey and Jett, for their endless support and sacrifice which have made my academic pursuits possible. I would also like to thank my extended family for their encouragement (and childcare). Thank you to my cohort members for their camaraderie and teamwork throughout a most challenging three-year journey. Last, but not least, thank you to my committee Chair, Dr. Laura Stanley, for your expertise, time and dedication enabling me to complete this dissertation. Thank you to my committee members, Dr. Watson, Dr. Martin and Dr. Subramaniam, for your invaluable contributions and commitment to this work. Thank you also to Dr. Richard Carrizosa and Dr. Jacob Arthur for your expertise and instruction regarding textual analysis.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LIST OF ABREVIATIONS

CSB	Cybersecurity Breach
CSR	Corporate Social Responsibility
IAF	Internal Audit Function
ICMW	Internal Control Material Weakness
IT	Information Technology
ITG	Information Technology Governance
MD&A	Management Discussion and Analysis
SEC	Securities and Exchange Commission
SOX-404	Sarbanes Oxley Act of 2002, Section 404
10-K	Annual Report Filing

CHAPTER 1: INTRODUCTION

As the number of annual breaches continues to increase (Verizon 2020), holistic understanding of an organization's IT Risk Culture and its impact on cybersecurity is of upmost importance. Accordingly, literature calls for research of IT risk management as a part of IT Governance (ITG) which should reflect a "structured, strategic approach that harmonizes needs for information with strategic decision-making that enables provision of investment, structures, people and relational mechanisms" (Wilkin and Chenhall 2010). The Risk IT Practitioner Guide (ISACA 2009a) coins this driving force for IT risk management the IT Risk Culture, which is based on management's behavior towards risk taking and its attitude towards regulation compliance and negative outcomes. In this dissertation I examine SEC mandated cybersecurity disclosures and other related disclosures to study IT Risk Culture and predominant risk response; specifically analyzing differential prediction of subsequent cybersecurity breach (CSB) incidents.

There are two major streams of information security research. The first stream examines defenses against cyber-attacks, while the second stream focuses on the economics of information security. This study focuses on the latter, exploring how IT Risk Culture relates to cost/benefit analysis and risk transfer via cybersecurity insurance, as well as other holistic actions to negate systemic cybersecurity risk. IT Risk Culture is part of IT Risk Management (**Figure 1**). Given IT or systems related risk is typically classified as operational in nature (Benaroch, Chernobai and Goldstein 2012), the IT Risk Culture permeates the organization's operations resulting in a greater potential to be more harmful than other elements of risk management (Jobst 2007). This study is the first to propose decisions specifically related to cybersecurity insurance reflect an organization's attitude related to the risk (i.e., IT Risk Culture).

The decision to transfer significant operational risk via insurance can have direct financial implications as well as reflect the internal attitude of an organization towards risk and responsibility. However, Richardson, Smith and Watson (2019) find very few material financial consequences for breached organizations, leaving costs effectively passed on to economically linked organizations and individuals. Their findings have an important implication: What type of organizational actions can be observed to evidence intention to mitigate cybersecurity incidents, given that the cost of breach may not be theirs solely to bear? In other words, to identify a company's behavior towards holistic risk management, Richardson et al.'s (2019) finding implies that a researcher must also look outside cybersecurity decisions.

To address the issue of identification, I draw upon corporate social responsibility (CSR) literature. CSR is an organization's efforts to surpass compliance by electing to engage in "actions that appear to further some social good, beyond the interests of the organization and that which is required by law" (McWilliams and Siegel 2006). Studies find that CSR activities are associated with improvements in the quality and reliability of information used for strategic planning, enterprise risk management, and effective internal control decisions (e.g., Casey and Grenier 2014). Accordingly, investments in CSR activities provide evidence of behavior towards holistic risk management that is outside of the cybersecurity decision. The inclusion of CSR activity introduces interdependent subsystems and is consistent with a systems focused IT Risk Culture.

In addition to CSR activity, the internal control environment, as a function of Sarbanes-Oxley Section 404 legislation of 2002 (SOX-404), also serves as a related component of a holistic approach to IT risk management. SOX 404 requires an extensive review and disclosure regarding controls over financial and operational systems and processes. IT controls are unique in that they extend into all types of control categories covered under SOX 404. As such, I evaluate the effective nature of the internal control system, as reported under SOX-404 legislation guidelines within the annual report (10-K), as an additional interconnected component of the IT Risk Culture of an organization.

Disclosures reflect an organization's internal information (Kasznik and Lev 1995) and the disclosure of information security risk has long been studied as a strategic measurement of an organization's risk culture (Gordon, Loeb and Sohail 2010). Signaling theory states that during situations of asymmetric information between organizations, costly signals can be sent and therefore create a separating equilibrium between those who are able to credibly signal and those who cannot (Spence 1978). Several studies demonstrate information differences between managers, investors, debtors, and customers. The inherent information asymmetry between parties leads to selective information sharing. Managers may selectively share positive information to improve the organizations valuation (Dye 1985) or selectively share negative information to reduce potential litigation costs (Skinner 1994). Studies extend signaling theory to organizational IT risks, where managers hold an information advantage about the actual IT risks facing the organization. Gordon et al. (2010) find a positive association between the value of an organization and managers' disclosure of information pertaining to the IT Risk Culture within the cybersecurity disclosure. In a related study, Wang, Kannan and Ulmer (2013) find the same disclosures are also related to CSBs. Through textual analysis, Wang et al. find organizations that disclose an active commitment to cybersecurity management are less likely to suffer a subsequent breach, whereas organizations with security risks and unresolved vulnerabilities are more likely to have a subsequent breach incident. Likewise, Berkman, Jona, Lee and Soderstrom (2018) evaluate a combined cybersecurity awareness measure, one component of which is sentiment of the disclosure. The authors find that, along with other attributes, organizations that convey a more positive tone in their cybersecurity disclosure demonstrate greater cognition of their cybersecurity risk and a more proactive approach to managing those risks. In contrast, organizations that convey a negative tone in their cybersecurity disclosure display lower cybersecurity awareness and exhibit greater cybersecurity vulnerability.

As such, prior literature demonstrates that the tone of the cybersecurity disclosure signals important elements of IT Risk Culture (i.e., cybersecurity awareness and vulnerability). I examine a logical extension of these findings. More specifically, I employ signaling theory to examine the association between the tone of the cybersecurity disclosure and the subsequent reported security incidents affecting the organization (i.e., cybersecurity breaches). Signaling theory is uniquely appropriate for this study since hackers are subject to information asymmetry regarding the organization's cybersecurity risks. In other words, there is a logical link between a current cybersecurity disclosure signal and subsequent attempts to breach the organization's cybersecurity.

In further tests, I examine the association between the textual sentiment of the cybersecurity risk disclosure, with and without the inclusion of cybersecurity insurance, and subsequent breaches. Current literature draws mixed conclusions as to the signal regarding risk sent by disclosure of cybersecurity insurance policy ownership. The decision to purchase cybersecurity insurance is unquestionably a transfer of risk. However, prior studies have not examined whether the purchase and disclosure of insurance concretely reflects a prevention/mitigation stance against cybersecurity risk or reflects a concession to remaining vulnerability. In this study, I examine the interactive effect between disclosure of cybersecurity insurance and overall cybersecurity risk disclosure tone and the likelihood of subsequent breach incident. The results of this additional analysis provide evidence that the two aspects of cybersecurity disclosure complement each other in signaling an organization's IT Risk Culture.

As an additional contribution, this study addresses a recent call for methodologically diverse accounting research (Stone 2018). Similar to other disciplines, the choice of methodology within accounting research depends on the nature of the question to predict or explain associations (Shmueli and Koppius 2009). Prior studies in accounting literature primarily use regression analysis to examine firm performance and stock returns as outcomes associated with textual contents of disclosures. In this study, I employ an unsupervised learning technique known as cluster analysis in an exploratory nature to identify classifications of IT Risk Culture – Risk Response. Utilizing previously identified attributes from the cybersecurity risk disclosure, sentiment and presence of cybersecurity insurance, as well as the interrelated organizational characteristics of SOX-404 internal control effectiveness and CSR activity, I identify varying IT risk profiles. Through cluster analysis, meaningful differences between groupings emerge, whereas different combinations of the five cluster variables (i.e., IT risk profiles) differentially predict subsequent CSB. I provide novel identification of IT Risk Culture classification, predominant risk response behavior and the likelihood of subsequent related outcomes.

In summary, this study has three specific goals. The first is to provide a model of how the contents of the cybersecurity risk disclosure signal the organization IT Risk Culture, specifically the role of cybersecurity insurance within IT Risk Culture. Secondly, this study furthers understanding of the association between disclosed CSR activity as a significant aspect of IT Risk Culture. Lastly, this study adds to the literature surrounding IT Risk Culture and identifies statistically unique IT risk profiles, or differences in predominant IT Risk Culture – Risk Response behavior. Findings suggest risk sharing/transfer predominant IT Risk Culture to be statistically likely to disclose subsequent CSB. Findings also suggest risk avoidant and risk reduction/mitigation predominant IT Risk Cultures not statistically likely to disclose subsequent CSB. Results of this study confirm IT risk management is not a siloed activity, but that IT risk must be evaluated from a holistic perspective. As a result of this dissertation, such IT risk profile classification ability will transform the cybersecurity risk assessment accuracy for investors, auditors, management and all economically linked organizations; improving prudence of investment decisions, audit engagement and fee setting decisions, risk evaluation of business partnership and data security confidence of customers and vendors, respectively.

In order to fulfill these objectives, chapter two reviews the IT risk and cybersecurity literatures. Chapter two also provides evidence that cybersecurity insurance and CSR represent a significant gap in the extant IT Risk Culture literature, as well as describes the theoretical models and related hypotheses. Chapter three provides details regarding the sample selection and data collection procedures, as well as a description of the research methodology. Next, empirical results and supplemental analyses are presented in Chapter four. Chapter five concludes this dissertation.

CHAPTER 2: LITERATURE REVIEW & HYPOTHESES

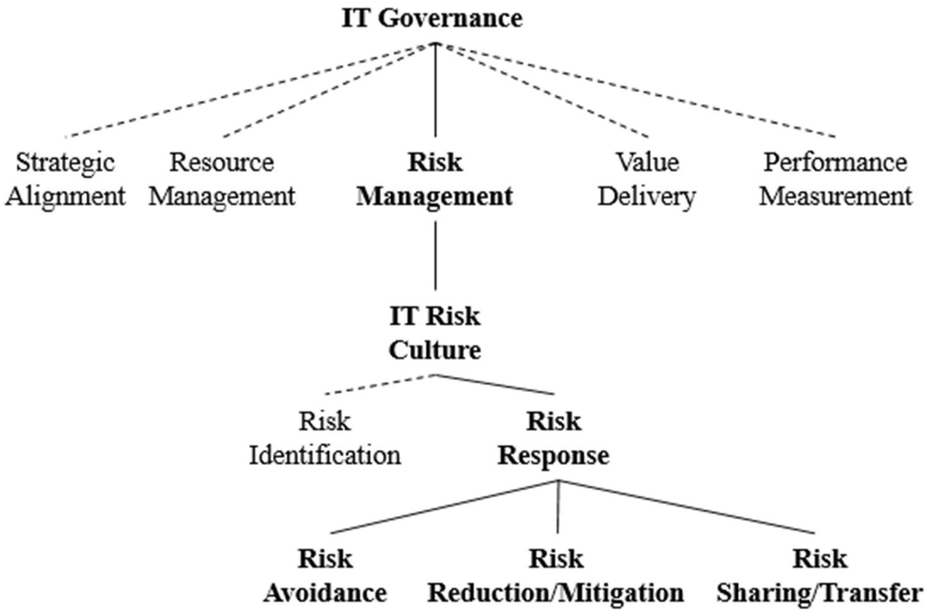
This literature review consists of three sections. In the first section, I review literature regarding cybersecurity risk management and its place within a general synthesized framework of IT Governance (ITG) (Figure 1). This dissertation contributes to the ITG literature by uniquely outlining the way in which multiple factors within the ITG structure, including IT risk management and IT Risk Culture, have a direct influence on cybersecurity outcomes within an organization. In the second section, I review cybersecurity breach literature. Within this section, I address existing literature related to subsequent outcomes, mitigation activities and predictive functions of cybersecurity breach, specifically those which are disclosed through the annual report. In the third, and last, section I discuss how the SOX 404 internal control environment and CSR activities within an organization have synergistic effects with cybersecurity risk disclosure components as they combine to create distinct classifications or profiles of IT Risk Culture, each uniquely predictive of cybersecurity breach. Hypotheses are included throughout the chapter as applicable.

2.1 IT Governance and Risk Culture

ITG was initially defined as the organizational and leadership structures and processes in place to ensure IT of an organization is able to sustain and extend the organization’s strategy and objectives (ITGI 2003). However, within this boundary condition, scholars note the importance of a holistic approach to ITG which describes a set of interdependent subsystems (processes, structures and relational mechanisms) that together deliver a powerful whole (Sambamurthy and Zmud 1999, Peterson 2004). More recently, ITG is delineated into five different focus areas; strategic alignment, risk management, resource management, value delivery and performance measurement (ITGI 2008). Wilkin and Chenhall (2010) highlight the importance of future investigation of IT risk management specifically related to the potential interplay between risk, security, privacy and alternative management strategies.

IT risk management is observed through actions of senior managers that communicate risk identification and risk response decisions such as risk avoidance, risk reduction/mitigation (Kumar 2002) and risk sharing/transfer (Risk IT 2009). It is the combination of these behaviors that contributes to the risk culture of an organization, defined as the predisposition of management towards taking risks (ISACA 2009, Pan, Siegel et al. 2017). As such, the IT Risk Culture of the organization is an important aspect of IT risk management and, therefore, ITG as well (**Figure 1**).

Figure 1: Theoretical Framework of ITG, IT Risk Management and IT Risk Culture



Risk culture, or attitude towards risk, is to a great extent dependent on the context in which risk is presented (Tversky and Kahneman 1992). Therefore, in considering IT Risk Culture as a component of ITG, it is imperative to consider the ultimate objective of ITG which is stated to be the creation of synergy between business and IT to obtain business value through

IT investments (Weill and Ross 2004). This repeated recognition of synergy as a necessary component to IT Risk Culture is a reflection of systems thinking (Kim 1999) in which organizations employ a holistic perspective to understand how interdependent components link together to determine overall performance (O'Donnell 2005). Utilization of systems thinking naturally leads to comprehensive IT risk management. Furthermore, in explaining how higher levels of analysis are achieved by holistic thinking, Gharajedaghji (2011) suggest three components must be analyzed to interpret system design: (1) structure of the system components and their association with other, (2) the function of each component as it relates to the outcome or results produced and (3) the process or sequence of activities necessary for generating desired outcomes. This systems approach echoes the call for interdependent subsystems which make up the holistic approach to ITG. As such, much is concluded about the ITG and IT Risk Culture of an organization through observation of a holistic approach to IT risk management.

2.2 Cybersecurity Risk

IT risk management includes several unique segments of consideration, including user management, enterprise architecture and cybersecurity (Debreceny 2013). Historical financial risk evaluation and subsequent management is unique in that the task has a certain point in time focus and an emphasis on materiality (No and Vasarhelyi 2017), while cybersecurity risk management is an aggregate of continuous parameters such as governance, control procedures, risk status, and data status (AICPA 2017a). Failure to successfully manage risk related to cybersecurity may result in cybersecurity breach (CSB).

Accordingly, cybersecurity risk management should consider a period of time and be based on multivariate estimates of different cybersecurity factors such as organizational characteristics and the nature of operations and information at risk (No and Vasarhelyi 2017). In an environment where there are countless and ever-changing threats to cybersecurity, an organization will never be able to achieve 100% risk coverage. As such, organizations must include a cost/benefit analysis in their decision process related to cybersecurity risk management (Gordon and Loeb 2002), as there is a point at which investments and risk management procedures related to cybersecurity exhibit diminishing returns.

The second component unique to cybersecurity risk management is the dual faceted nature of options for management; whether it be prevention and mitigation efforts or risk transfer (Bodin et al. 2018). Scholars find the association between IT investment, IT risk management and resulting outcomes, such as cybersecurity breach, and note organizations with higher levels of IT investment governance at the board level are more likely to maximize the contribution of their IT investments to organization value (Ali, Green and Robb 2015). These IT investments related to prevention of cybersecurity breach include firewalls, intrusion detection systems, encryption, employee training, etc. In addition to the influence on IT investment decisions, the IT Risk Culture of the organization also influences the purchase of cybersecurity insurance to transfer some of the cybersecurity risks associated with potential future breaches (Herath and Herath 2008).

2.3 Cybersecurity Risk Disclosure

Beginning in 2011, the Securities and Exchange Commission (SEC) has made a series of disclosure guidance regarding cybersecurity with the discussion of what, if any, disclosure public companies should provide in the risk-factor section of 10-k filings (SEC 2011). The interpretive guidance provided by the SEC primarily requires organizations to inform investors about material cybersecurity risks and incidents in a timely fashion. In a study prior to the 2011 SEC guidance, Gordon et al. (2010) find that the then voluntary disclosure of cybersecurity vulnerabilities and proactive security measures had a significant positive impact on an organization's stock price. However, subsequent studies have since focused on the informative nature of the now mandatory cybersecurity disclosures, noting mixed findings. Hilary, Segal and Zhang (2016) find no significant association between an organization's prior cybersecurity risk disclosure and the market reaction post cybersecurity breach. However, in a slightly more recent study by Li, No and Wang (2018) authors observe a dissimilar association in which both the presence and length of cybersecurity risk disclosure are predictive of future security incidents, which according to extant theory should be associated with unfavorable market reaction.

Cybersecurity risk disclosure contents are of increasing importance (Cheong, Cho, No and Vasarhelyi 2019) to understand the relationship between the organization IT Risk Culture and subsequent outcomes. A recent study by Berkman et al. (2018) creates a measure of organization level cybersecurity awareness as evidenced by the extent and relevance of cybersecurity disclosures. The study observes a positive association between cybersecurity awareness and market valuation, as well as a positive association between negative tone in cybersecurity disclosures and lower market valuation (Berkman et al. 2018). Most importantly, the study provides evidence that cybersecurity disclosures provide the means to measure key components of IT Risk Culture, awareness and sentiment related to cybersecurity through textual analysis.

Table 1: Excerpts from Cybersecurity Risk Disclosure – Item 1A Risk Factors

"***The operation of the Company's business is heavily dependent on its information systems.*** We depend on a variety of information technology systems for the efficient functioning of our business and security of information. Much information essential to our business is maintained electronically, including competitively sensitive information and potentially sensitive personal information about customers and employees. Our insurance policies may not provide coverage for security breaches and similar incidents or may have coverage limits which may not be adequate to reimburse us for losses caused by security breaches. We also rely on certain hardware and software vendors to maintain and periodically upgrade many of these systems so that they can continue to support our business. The software programs supporting many of our systems were licensed to the Company by independent software developers. The inability of these developers or the Company to continue to maintain and upgrade these information systems and software programs could disrupt or reduce the efficiency of our operations. In addition, costs and potential problems and interruptions associated with the implementation of new or upgraded systems and technology or with maintenance or adequate support of existing systems could also disrupt or reduce the efficiency of our operations or leave the Company vulnerable to security breaches. We also rely heavily on our information technology staff. If we cannot meet our staffing needs in this area, we may not be able to fulfill our technology initiatives or to provide maintenance on existing systems." FY 2016

*"**Failure to maintain the security of our business, customer, employee or vendor information or to comply with privacy laws could expose us to litigation, government enforcement actions and costly response measures, and could materially harm our reputation and affect our business and financial performance...***A significant security breach of any kind experienced by us or one of our vendors, which could be undetected for a period of time, or a significant failure by us or one of our vendors to comply with applicable privacy and information security laws, regulations and standards could expose us to risks of data loss, litigation, government enforcement actions, fines or penalties, credit card brand assessments, negative publicity and reputational harm, business disruption and costly response measures (for example, providing notification to, and credit monitoring services for, affected individuals, as well as further upgrades to our security measures) which may not be covered by or may exceed the coverage limits of our insurance policies, and could materially disrupt our operations. Any resulting negative publicity could significantly harm our reputation which could cause us to lose market share as a result of customers discontinuing the use of our e-commerce and mobile applications or debit or credit cards in our stores or not shopping in our stores altogether and could materially adversely affect our business and financial performance." FY 2019

2.3.1 Cybersecurity Insurance Disclosure

Cybersecurity insurance, typically held at the discretion of IT risk management, is considered a non-IT related security investment factor and is defined as insurance coverage designed to mitigate losses from a variety of cyber incidents; including data breaches, network damage and cyber extortion (Liu, Bose and Luo 2014) and even social media risk (Demek, Raschke, Janvrin and Dilla 2018). Due to the frequent mismatch between technological controls and the skill of cybersecurity threat, models suggest there to be a residual cybersecurity risk that is transferrable through cybersecurity insurance (Bandyopadhyay, Mookerjee and Rao 2009). Since its entrance as a new product within insurance markets researchers have voiced concerns over cybersecurity insurance, including issues of pricing, adverse selection and moral hazard (Gordon, Loeb and Sohail 2003). However, given the constraints previously discussed related to cybersecurity risk, it is with vast justification a valid component of IT risk management.

Theoretically, cybersecurity insurance should be purchased after the IT risk assessment concerning information security is completed and management identifies any remaining areas of vulnerability. IT risk management then evaluates available policies and determines the policy to best cover remaining risk via two levels of coverage; first party coverage, covering for costs due in response to loss of clients' or employees' private information, and third-party coverage, covering for legal defense costs including lawsuits filed by consumers and other businesses (Liu et al. 2014). Although the economics of cybersecurity insurance pricing are not as sophisticated as more mature insurance products, the ability to transfer cybersecurity risk is one deserving of research attention.

As cybersecurity insurance is considered a form of cybersecurity investment, it has been studied from that perspective to a moderate extent. However, as a single construct separate from the organization wide IT or cybersecurity investment amount for any given accounting period, cybersecurity insurance as an IT risk management decision reflective of IT Risk Culture is yet to be empirically evaluated. Existing empirical papers which study cybersecurity insurance focus on either the pricing of the insurance policies and the optimum policy selection process for IT risk management within an organization or risk advisors guiding the organization (Bodin et al. 2018) or the value of information sharing amongst cybersecurity insurance market (Gordon, Loeb, Lucyshyn and Zhou 2015). There are yet to be any empirical studies which evaluate the association between disclosed cybersecurity insurance as a component of cybersecurity risk disclosure and positive outcomes, such as market valuation, or negative outcomes, such as cybersecurity breach.

In line with the most recent SEC guidance related to cybersecurity risk disclosure, which specifically highlights the significance of cybersecurity insurance as a component of cybersecurity risk management (SEC 2018), the purchase and disclosure of cybersecurity insurance reflects the IT Risk Culture. Interestingly, Liu et al. (2014) suggest that an organization willing to purchase such insurance would also implement proper preventative measures to ensure its usage will never be necessary and propose a positive effect on organization outcomes regarding information security.

2.4 Cybersecurity Breach

According to the AICPA, cybersecurity is defined as “the process of applying security measures to ensure confidentiality, integrity and availability of data” (AICPA 2017). Therefore, cybersecurity breach (CSB) occurs when penetration of the technologies, processes and practices that safeguard and assure the protection of an organization’s information systems (No and Vasarhelyi 2017) occurs. CSB results in compromise of the confidentiality, integrity and availability of data organization wide. Relevant CSB extant literature stems from the accounting information systems and management information systems disciplines. I classify CSB extant research into the following three categories: subsequent consequences, mitigation efforts post breach, and predictive measures prior to incidence (**Table 2**).

Table 2: Cybersecurity Breach (CSB) Literature

Category	Relevant Articles	Constructs Related to CSB
Subsequent Outcomes	19	Financial and reputational impact Changes in audit fees and risk assessment Changes in market value of breached organization Impact on economically linked organizations
Mitigation Efforts	10	CSB disclosure Management responsibility acceptance IT investment SOX-404 internal control process revision CEO/CIO turnover IT Governance changes
Predictive Measures	6	Risk tolerance of executives Board level characteristics Disclosure of trade secrets Cybersecurity risk disclosure content and length

2.4.1 Subsequent Outcomes Post CSB

The most studied aspect of CSB is the subsequent outcomes associated with past breach including financial and reputational impact on the breached organization, changes in audit fees and risk assessment, changes in market value of the breached organization, and the impact of breach on economically linked organizations. Extant literature finds that with each occurrence of CSB, impacted organizations are subject to a series of repercussions enabling management and external users the predictive ability to deduce outcomes likely to arise post CSB.

As all systems are potential victims of cyberattacks (Ransbotham and Mitra 2009), consequently all companies may potentially experience an outcome associated with CSB. Extant research is largely concerned with the economic impact of data breaches, focusing on the breached organization. Research generally finds a negative economic effect of CSB (Gordon, Loeb and Zhou 2011; Steinbart, Raschke, Gal and Dilla 2013; Steinbart, Raschke, Gal and Dilla

2018). Specific findings include negative outcomes on a variety of accounting measures including future sales, return on assets, return on equity, cash flow volatility, and long-term debt (Kamiya, Kang, Kim, Mildonis and Stulz 2018), and research and development expenditures (Bianchi and Tosun 2019).

Additional consequences of CSB include damaged relationships with various related parties, including investors. For example, studies using event study or other empirical techniques find a significant, negative impact of CSB on an organization’s market value. These studies examine a variety of factors including market reaction on the day of disclosure as opposed to reaction over time (Acquisti, Friedman and Telang 2006); market reaction based on the type of information breached (i.e. confidential or not confidential information) (Campbell, Gordon, Loeb and Zhou 2003); impact of market returns for the breached organization and related organizations not actually attacked via the information transfer effect (Ettredge and Richardson 2003, Cavusoglu, Mishra and Raghunathan 2004); and classification of primary effect of breach (i.e., confidentiality, availability or integrity) (Gordon et al. 2011).

More recently, research is using textual analysis to examine disclosure contents. Wang et al. (2013) study the association between textual contents of information security breach reports by the media and changes in the affected organization’s stock price. Observations include market consensus about the negative impact of the reported security incident on an organization’s value; occurring primarily when the textual contents contain greater detailed information as opposed to a lack of specific information regarding the breach. This study was one of the first to empirically validate the impact of textual information pertaining to CSB and the association to various outcomes.

After a CSB, audit fees and risk assessment procedures significantly change. Observed increases in audit fees may be mediated by other factors directly caused by CSB, such as increase in business risk or increase in IT investment and therefore IT complexity. Li, No and Boritz (2017) are the first to find a significant positive association between increases in audit fees and hacking cyber incidents, but not other types of CSB incidents. Additional subsequent studies find further positive associations between CSB and audit fees (Lawrence, Minutti-Meza and Vyas 2018, Yen, Lim, Wang and Hsu 2018, Rosati, Gogolin and Lynn 2019, Smith, Higgs and Pinsker 2019). However, the associations are not exclusively found post breach, but also prior to breach. This recurrent observation supports research investigating the organizational characteristics that are predictive of future CSB; particularly, characteristics the audit firm would be privy to such as IT Risk Culture and the effectiveness of SOX 404 control environment.

Yen et al. (2018) specifically note the importance of IT in an organization’s operating environment, providing evidence of the association between information integrity, reliability of financial reporting, and overall organization reputation. Research pertaining to the reputation management or mitigation strategies post CSB is critical and growing in depth. Curtis, Carre and Jones (2018) find consumer trust is more strongly influenced by what has happened as opposed to what will happen and assurances about the future security measures. These findings support the need for additional research to determine effective breach prevention strategies.

Unlike extant literature, in a recent study Richardson et al. (2019) find contradictory evidence suggesting very few consequences for breached organizations. Through the use of one consistent sample spanning a longer period of time and representing a much larger population, the study finds that most organizations do not exhibit any discernable impact on financial performance, audit fees or other fees, or internal control weaknesses. While these findings are intriguing, the frequency of breaches continue to increase (Verizon 2020) and the existence of cost due to breach is irrefutable. Studies such as Richardson et al. (2019) and Amir, Levi and Livne (2018) question whether the true cost of CSB is shouldered by breached organizations or spills over to individuals and economically linked entities.

2.4.2 Mitigation Efforts Post CSB

A second delineation of research related to CSB includes the study of actions of the breached organization immediately following CSB. Mitigation strategies include reactive management activity such as CSB disclosure, management responsibility acceptance, IT investment, SOX 404 internal control procedure revision, CEO/CIO turnover, and changes to IT Governance structures. Related studies observe the associations between the CSB and mitigation strategies from both the predictive and prescriptive perspectives; enlightening investors as to which actions from management to expect to see post various types of CSB and informing management of best practices to implement for optimal future outcomes post CSB.

In a February 2018 pronouncement, the SEC stated the critical importance of organizations to timely disclose material cybersecurity incidents (SEC 2018). According to extant literature, the timing of CSB disclosure has significant impact on the market's reaction (Campbell et al. 2003, Gatzlaff and McCullough 2010, Gordon et al. 2010). Specifically, Cheng and Walton (2019) find favorable investor response from initial disclosure of breach made timely by the organization, as opposed to unfavorable investor response when the disclosure is delayed or first made by an external source. The impact of IT Risk Culture on the decision to disclose information on material CSB incidents is significant, as managers have incentives to withhold negative information and investors cannot discover most CSB incidents independently (Amir et al. 2018). Evidence suggests managers have a propensity to not disclose negative information below a certain threshold and to withhold information on the more severe attacks, unless investors already suspect a high likelihood of a CSB incident. Therefore, if investors or external auditors were able to accurately predict the likelihood of CSB incident, this prediction would enable conclusions regarding transparency of IT risk disclosure and association with future CSB, creating a clear glance into the IT Risk Culture of the organization.

Furthermore, studies demonstrate an association between the level of management responsibility acceptance via CSB disclosure and investor reactions. In a 2018 study, Tan and Yu observe from investors the assignment to management a higher responsibility for internal CSB and lesser responsibility for external CSB. These findings extend the work of Wolfe, Mauldin and Diaz (2009) who are the first to observe, within an IT context, accepting more responsibility is not always more effective than accepting less responsibility. Conclusions from this research suggest the cybersecurity risk disclosure conveys management attitude towards responsibility acceptance, the latter of which is a key component of IT Risk Culture - Risk Response (**Figure 1)**.

The occurrence of CSB can signal to the board of the breached organization a lack of oversight, resulting in a number of IT risk oversight changes including the formation of an IT Governance committee at the board level or changes made to the CIO or CISO executive position. For example, breaches caused by system deficiency are found to increase CIO turnover likelihood by 72 percent (Banker and Feng 2019). Additionally, Higgs, Pinsker, Smith and Young (2016) suggest organizations with breach risk or past breach may consider board-level governance strategies, such as forming a technology committee, as a way of mitigating negative market returns as the creation of this committee signals the attempt to manage risk and causes an increase in favorable investor reaction over time. Likewise, a CSB incident may send the same signal to audit firms of breached organizations, as organizations reporting past CSB are associated with increased audit fees (Smith et al. 2019). Expanding upon previously discussed conclusions, the work of Smith et al. (2019) also find the presence of board-level committees help to mitigate this audit fee premium.

2.4.3 CSB Predictive Functions

Arguably the least developed stream of research related to CSB includes the study of variables predicting CSB. Authors study what internal and external factors predict future CSB. This knowledge is valuable to IT risk management, internal and external assurance functions, investors and economically linked organizations.

Kwon, Ulmer and Wang (2013) find the existence of an IT executive within a top management team to be negatively associated with the possibility of CSB. The authors also find the amount of behavior-based compensation and pay differences among IT and non-IT executives are negatively associated with the likelihood of CSB. In a subsequent study, Feng and Wang (2019) specifically study risk tolerance of executives and find the level of CIO risk aversion to be negatively associated with CSB incidents, but only incidents of internal and non-hack breaches. Furthermore, they find the association strengthened when other members of management exhibit risk aversion.

While IT Governance encompasses actions resulting from the top management team, it is predominately driven by board-level characteristics. Accordingly, Higgs et al. (2016) find that organizations with newly established board-level technology committees are more likely to have reported breaches in the same year as committee origination than organizations without the committee; however, this association decreases over time with maturity of the board-level technology committee. As such, characteristics of the board and executive management predict the vulnerability and likelihood of future CSBs.

Organizations disclose a wide range of information, both direct and indirect, about the vulnerability of the organization to CSB through the annual report (10-K). An indirect disclosure of seemingly unrelated information can be found to have a direct association with a subsequent breach. For example, Ettredge, Guo and Li (2018) were the first to observe an association between organizations which disclose the existence of trade secrets and subsequent CSB. The authors specifically find that it is the disclosure content, not simply the existence of trade secrets, that increases the likelihood of being a target for cyber-attack. These findings highlight the importance of a holistic approach to IT risk management, as IT security can be threatened by many different aspects of the organization.

Gordon et al. (2010) find the voluntary disclosure of items pertaining to information security is positively associated with the market value of an organization, and as a result are the first to confirm the ability of IT risk disclosure to signal information related to IT governance. Extending this work, Wang et al. (2013) utilize textual analysis to analyze the nature of the information security disclosure as either positive or negative, i.e., containing primarily statements of either risk mitigation or risk vulnerability, and the predictive ability of future CSB. The authors develop a decision tree model to classify the contents of the information security disclosure and find that risk mitigation disclosures are less likely associated with breach announcements, while risk vulnerability disclosures are more likely to predict CSB announcement. These findings support the conclusion that signaling a certain position in IT risk management has predictive ability for organizational outcome, i.e., realization of the event.

Building on theoretical propositions from Gordon and Loeb (2002), Tanaka, Marsuura and Sudoh (2005) empirically validate the association between an organization's decisions regarding IT security investment and vulnerability to CSB. Given the cost-benefit analysis that must be considered by IT risk management, this is an understudied aspect of cybersecurity risk management. Tanaka et al. (2005) prescribe a method for using the level of information security investment to predict vulnerability of the organization. They find in cases of medium-high vulnerability, information security investment is cost-effective and therefore likely to result in IT security investments. Accordingly, these findings can be used to expand that of Wang et al. (2013) in that IT investment does signal vulnerability and perhaps also likelihood of subsequent breach announcement, while also decreasing the probability due to purchased preventative control.

Directly related to the investigation of how the cybersecurity risk disclosure predicts the likelihood of future CSB, Li et al. (2018) find a number of relevant associations. Prior to the 2011 SEC cybersecurity disclosure guidance, authors find the association of then voluntary cybersecurity risk disclosure with subsequent CSB (Li et al. 2018), however this association disappeared in the post-guidance period as organizations of varying levels of cybersecurity vulnerability all included risk disclosure for compliance measures. Interestingly, post SEC guidance, the length of the cybersecurity risk disclosure is positively associated with subsequent cybersecurity incidents, risk disclosures are less informative overall, and disclosed content changes. These conclusions suggest the need for additional research of the risk disclosure contents in order to understand what specific details included, or not, have a positive association with subsequent CSB.

In a subsequent study by Berkman et al. (2018) authors utilize textual analysis to examine the content of cybersecurity disclosures, noting a novel measure of cybersecurity awareness on behalf of IT Risk Culture, and providing evidence to suggest cybersecurity disclosures in the post 2011 guidance period are not merely boilerplate disclosures, but provide value relevant information for investors. This measure of cybersecurity awareness captures the extent and relevance of disclosures and shows that the market positively values cybersecurity awareness. Likewise, lower levels of cybersecurity awareness in the cybersecurity disclosures are associated with lower market values.

2.5 Signaling Theory and Cybersecurity Risk Disclosure

As discussed, the cybersecurity risk disclosure provides direct insight into the IT Risk Culture of an organization. While extant literature finds positive association between elements of the cybersecurity risk disclosure and subsequent market valuation, this study focuses on what the cybersecurity risk disclosure components signal about the IT Risk Culture of the organization and therefore likelihood of realization of event to better understand the market response.

Given that prior literature suggests internal information is often reflected in the nature of the disclosure (Li 2008), like Wang et al. (2013), this paper studies the relationship between the nature of information security disclosures and the reported security incidents affecting the organizations. Commonly used within disclosure literatures, signaling theory states that when parties have asymmetric information, costly signals can be sent to create a separating equilibrium between those who can credibly signal and those who cannot (Spence 1978). In a similar manner, management (and in turn, the board) has private information about the organization’s cybersecurity risk, which is a necessary condition for a signal (Higgs et al. 2016). Stiglitz (2000) highlights two broad types of information where asymmetry is particularly important:

information about quality and information about intent. Contents of the cybersecurity risk disclosure signal the quality of information, or transparency of the risk communication, as well as the true intention to transfer the unavoidable CSB risk through insurance coverage. This study's hypotheses are grounded in signaling theory; specifically, the information within the cybersecurity risk disclosure is a signal sent by management about the IT Risk Culture and ability of the organization to successfully prevent future cybersecurity breach incidents. Furthermore, extant research finds that the information signaled via cybersecurity risk disclosure elicits response by third parties, including cybersecurity hackers and investors.

While Gordon et. al. (2010) are the first to confirm the ability of cybersecurity risk disclosure to signal information related to IT governance, Wang et al. (2013) confirm the signaling of a certain IT Risk Culture of an organization to predict organizational outcome, i.e., realization of the event. Since the cybersecurity risk disclosure contains qualitative information, qualitative analysis is utilized to analyze measures of risk, vulnerability, cybersecurity awareness and sentiment; each reflective of IT Risk Culture. Accordingly, this study analyzes components of the cybersecurity disclosure to predict classifications of IT Risk Culture and likelihood of subsequent CSB.

2.5.1 Sentiment of Cybersecurity Disclosure Association with Cybersecurity Breach

In the same manner that Wang et al. (2013) study subsequent outcomes related to the Gordon et al. (2010) model of association between cybersecurity risk disclosure and market valuation, there is yet to be a study of subsequent outcomes related to the Berkman et al. (2018) model of association between cybersecurity awareness and market valuation. In this study, a primary component of measuring cybersecurity awareness is the calculation of disclosure sentiment. In both Berkman et al. (2018) and this dissertation, text-based or textual sentiment is defined as the degree of positivity or negativity in tone and is thought to capture an objective reflection of conditions within organizations (Kearney and Liu 2014). Particularly, textual sentiment is useful for interpreting management's perspective according to the initial design of the MD&A section of the annual report (Feldman, Govindaraj, Livnat and Segal 2008). Building on this research, I use textual analysis of cybersecurity risk disclosure to evaluate IT Risk Culture.

Results from Berkman et al. (2018) indicate higher (lower) levels of cybersecurity awareness are associated with positive (negative) measures of disclosure sentiment, and subsequently higher (lower) subsequent market valuation. Furthermore, Wang et. al (2013) state a distinction between two types of internal information may be recognized when the disclosed risks are realized. Extending extant research, I propose an IT Risk Culture with a proactive approach to risk response, supported by positive sentiment of cybersecurity risk disclosure, signals the ability to prevent future cybersecurity breach. Likewise, I also propose an IT Risk Culture with a reactive approach to risk response, supported by negative sentiment of cybersecurity risk disclosure, signals the inability to prevent future cybersecurity breach. Formal hypotheses to follow:

H1a: The positive sentiment of cybersecurity risk disclosure is negatively associated with the likelihood of subsequently reported cybersecurity breach.

H1b: The negative sentiment of cybersecurity risk disclosure is positively associated with the likelihood of subsequently reported cybersecurity breach.

2.6 The Moderating Impact of Cybersecurity Insurance Disclosure in Disclosure Sentiment

In an attempt to capture a comprehensive picture of IT Risk Culture from components in the cybersecurity risk disclosure, an analysis should encompass both the organization's attitude toward risk as well as management's behavior towards risk management (ISACA 2009). Cybersecurity insurance purchase and disclosure is a measureable risk response behavior and a function of IT Risk Culture. However, a sparse amount of research has been conducted on how cybersecurity insurance affects an organization's risk mitigation efforts and results are mixed (Gordon et al. 2003, Bolot and Lelarge 2009). While the purchase and disclosure of cybersecurity insurance is one such behavior reflective of IT Risk Culture, this study is the first to propose an association between purchased and disclosed cybersecurity insurance and disclosure sentiment, specifically proposing the presence of cybersecurity insurance to be an affirmation of disclosure sentiment and IT Risk Culture. The disclosure of cybersecurity insurance is likely multidimensional, encompassing the level of cybersecurity vulnerability of the organization and therefore the disclosure of cybersecurity insurance is an important factor that strengthens the signal of positive or negative sentiment and likeliness of the organization to incur subsequent CSB.

An important research question is this: How does the disclosure of cybersecurity insurance influence the association between CSB determinants and subsequent outcomes? Studies addressing this question might uncover significant differences in disclosure sentiment and support requirements that depend upon the presence of disclosed cybersecurity insurance to generate important theoretical insights regarding risk of CSB, such that cybersecurity insurance is a function of risk culture signaled via disclosure sentiment. In the theoretical model of cybersecurity disclosure prediction of CSB (**Figure 2**), this study proposes that the cybersecurity disclosure sentiment will be a stronger predictor of CSB with the presence of cybersecurity insurance in the disclosure, whereas the negative relationship between positive sentiment and

CSB along with the positive association between negative sentiment and CSB will each be strengthened.

Underlying this rationale that cybersecurity insurance disclosure is an important moderator is the recognition that the motivation for risk transfer can vary amongst differing IT Risk Cultures. Cutler and Zeckhauser (2004) note cybersecurity insurance is most effective in cases where “losses are common enough to be of concern but not frequent enough to be routine”. From this perspective, like other forms of insurance, cybersecurity insurance can result from good corporate strategy, preventing the need for a large sum on money to be appropriated for self-insurance purposes (Mukhopadhyay, Chatterjee, Saha, Mahanti and Sadhukhan 2013). For example, previously discussed areas of vulnerability can be identified through cybersecurity risk assessment. Organizations make a series of subsequent choices; first, whether to purchase cybersecurity insurance and second, whether to disclosure if such insurance is held. Extant literature considers cybersecurity insurance a viable complimentary tool which organizations can use to hedge against cybersecurity risk, particularly after investing in technology security systems and demonstrating effective systems of internal control (Mukhopadhyay et al. 2019). This dissertation hypothesizes that the signaling of positive sentiment reflects a proactive IT Risk Culture; likewise, actions identified by Mukhopadhyay are also indicative of a proactive IT Risk Culture. Therefore, when cybersecurity insurance is purchased and disclosed the negative association between positive sentiment and likelihood of future CSB is strengthened.

In contrast, existing literature previously discussed alternatively suggests an association between IT investment and vulnerability of the organization related to cybersecurity risk, in which instances IT investment does include cybersecurity insurance. Drawing upon the findings of Berkman et. al. (2018), a positive (negative) sentiment expressed in cybersecurity disclosure is associated with cybersecurity awareness and the ability (inability) to prevent cybersecurity breach, i.e., absence (presence) of vulnerability. Borrowing from economics based literature, Ehrlich and Becker (1972) distinguish the insured's action to reduce the size of a loss (self-insurance) from the action to reduce the probability of the loss. The authors find that an insurance policy written by a third party tends to substitute self-insurance, but it can complement self-protection if the probability of loss is large. In this instance, when cybersecurity insurance is disclosed midst negative sentiment, the disclosure signals a stronger self-protection IT risk culture due to probability of loss. Therefore, under the condition that an organization discloses cybersecurity insurance, the positive association between negative sentiment, related to the reactive nature of the IT Risk Culture, and likelihood of future CSB is strengthened. Formal hypotheses to follow:

H2a: The presence of cybersecurity insurance coverage within the cybersecurity risk disclosure strengthens the negative association between positive disclosure sentiment and the likelihood of subsequently reported cybersecurity breach.

H2b: The presence of cybersecurity insurance coverage within the cybersecurity risk disclosure strengthens the positive association between negative disclosure sentiment and the likelihood of subsequently reported cybersecurity breach.

2.7 Classification of IT Risk Culture Determinants

Cybersecurity risk management should be based on multivariate estimates of different cybersecurity factors, including organizational characteristics (No and Vasarhelyi 2017). Therefore, in addition to the information reflected in the cybersecurity risk disclosure signaling the IT Risk Culture of an organization, additional observed characteristics of an organization comprise a more complete classification of IT Risk Culture as it relates to likelihood of subsequent CSB. The following sections provide a review of the literature and suggest that the internal control environment and the corporate social responsibility practices of an organization are necessary attributes for IT Risk Culture classification.

2.7.1 Internal Control Environment and IT Risk Culture

Corporate information security disclosure activities have received much greater focus since the passage of the Sarbanes-Oxley (SOX) Act of 2002 legislation (Gordon et al. 2006). The SOX Act of 2002 solidifies the importance of information systems controls by requiring management and auditors to report on the effectiveness of internal controls over the financial reporting component of the organization's management information system (Li, Peters, Richardson and Watson 2012). In this way, the external audit opinion over internal control effectiveness provides evidence of the ability of management to operationalize the IT Risk Culture signaled via cybersecurity risk disclosure.

In response to SOX legislation, many organizations are realizing the importance of their IT governance strategies and the impact that their governance strategies can have on their organization's success (Bowen, Cheung and Rohde 2007). Klamm et al. (2012) find account-level and entity-level financial reporting deficiencies occur at a significantly higher rate in SOX 404 reports with at least one IT material weakness (MW) than in reports with only non-IT MWs. Furthermore, the IT control environment has the strongest impact on future MW of all types. These findings suggest effective corporate governance across IT domains is pivotal in establishing sound internal controls (Klamm et al. 2012). Accordingly, strong ITG is likely found to be associated with effective systems of internal control.

Cybersecurity is coined an "umbrella concept" that encompasses information security and information assurance (No and Vasarhelyi 2017). Steinbart et al. (2012) state that the internal audit and information-security functions should co-operate synergistically, further supporting the claim that a synergistic IT risk culture is likely to negate cybersecurity instances. Accordingly, Rahimian, Bajaj and Bradley (2016) create a model which can be used to help bridge the expertise and perspective gap between the IT function and internal audit, which is the foundation which IT risk management stands upon. Through empirical testing of their model, Rahimian et al. (2016) identify the importance of a shared view of the significance of in-place and missing information security controls.

The internal audit function (IAF) is of extreme importance when analyzing the effectiveness of a corporations' internal control structure. Extant literature finds the extent to which an IAF completes a cybersecurity audit is significantly and positively associated with the internal audit competence related to governance, risk and control (Islam, Farah and Stafford 2018). A further conceptual study concludes the significance of formal documentation of cyber controls and notes the importance of the IAF in this process due to visibility across the organization (Kahyaoglu and Caliyurt 2018). Lastly, a 2018 study finds the quality of the relationship between the IAF and IT management functions has an inverse association with the number of reported internal control weaknesses and incidents of non-compliance. The number of security incidents detected both before and after material harm incurred by the organization is also inversely associated with the quality of IAF-IT relationship (Steinbart et al. 2018). Thus, for organizations that approach IT risk management from a systems perspective, their IT Risk Culture is likely to demonstrate understanding of the related nature of both functions and result in effective IT internal control environments.

Extant literature echoes the cost-benefit analysis component to IT risk mitigation and IT control investment (Wallace, Lin and Cefaratti 2011). IT control environments now have a significant impact on the organization as investment in cloud computing technologies continue to increase. Findings also suggest IT investment may increase internal control risk due to increased system complexity (Han, Rezaee, Xue and Zhang et al. 2016). As such, IT governance able to identify specifically which IT vulnerabilities and risks are associated with the most damage to the organization is of critical importance (Kim, Richardson and Watson 2018).

Extant literature also finds a significant association between IT internal control quality and market valuation (Stoel and Muhanna 2011). Stoel and Muhanna (2011) confirm the significance of IT-induced risk due to faulty IT controls as opposed to any marginal value provided by superior IT usage. For certain IT controls related to cybersecurity, even a single incidence of failure of the control could be an indicator of an ineffective system of controls related to cybersecurity, permitting material incidents to occur (Li, No, Cheong and Halterman, 2019). IT controls are unique in that they extend into multiple control type categories, financial and operational controls. Additional research suggests the disclosure of IT internal control material weakness in an organization’s annual report (10-K) is associated with a dramatic, negative impact on the organization and its leadership (Kim et al. 2018). As such, the broad study of the internal control environment as a whole, with a focus on understanding the IT governance structure of an organization from a holistic perspective, should lend novel insight into the likelihood of the effective control environment to protect the organization against cybersecurity incidents.

Amir et al. (2018) state that organizations with stronger corporate governance are less likely to withhold negative news from their investors, considering stronger governance is associated with stronger fiduciary responsibility. Using material weakness of internal controls for financial reporting reported under Section 404 of the Sarbanes-Oxley Act of 2002, the study was able to measure governance strength and therefore fiduciary responsibility as an element of an organization’s risk culture. Cybersecurity breaches may be an indicator of material weakness in controls across the company, which may be missed or reported later than sooner (Lawrence et al. 2018). Accordingly, the effectiveness of the internal control system has a direct influence on the strength of signals sent about an organization’s risk culture via information security disclosure.

2.7.2 Corporate Social Responsibility and IT Risk Culture

The cybersecurity activities of a given organization affect not only the probability of that organization experiencing a CSB, but also the probability that other organizations (and individuals) suffer breach and economic consequence (Gordon, Loeb, Lucyshyn and Zhou et al. 2014). The primary objective of Gordon et al. is to investigate the magnitude of underinvestment in cybersecurity activities by a private sector organization that considers only its private costs and benefits without regard to externalities. In doing so, the authors find that a risk-neutral organization’s social optimal investment in cyber security increases by no more than 37% of the expected externality loss. As such, unless organizations consider the costs of breaches associated with externalities in addition to their private costs resulting from breach, underinvestment in cybersecurity activities is certain; including cybersecurity insurance.

While the risk of a cybersecurity breach is one that must be managed, many studies question whether a cybersecurity breach is indeed harmful to the organization (Amir et al. 2018, Richardson et al. 2019). However, these studies measure loss from cybersecurity breach in terms of direct financial repercussions. Richardson et al. (2019) specifically find no evidence of a negative impact on market returns, financial performance, or audit fees. Instead, the authors propose the true cost of data breach is incurred by individuals and economically linked organizations.

As such, extant literature is yet to study the association between organizations which intentionally demonstrate consideration for all stakeholders through Corporate Social Responsibility (CSR) and effective cybersecurity risk management. CSR activities are associated with improvements in the quality and reliability of information used for strategic planning, enterprise risk management and more effective internal management control decisions (Casey and Grenier 2014). Assurance over these activities is the object of repeated suggestions from research, specifically related to the SOX 404 internal control audit, such that a broadened scope would encourage companies to take cybersecurity seriously and better protect the private information of customers and employees (Richardson et al. 2019).

Ballou, Casey, Grenier and Heitger (2012) are the first to measure the extent to which organizations are embedding CSR activity into their strategic decision making and found, even after obtaining independent assurance on CSR activities, organizations may or may not choose to disclose such information. However, more recently, voluntary disclosures of leading nonfinancial information (i.e., CSR) have been observed as increasing in volume and perceived as increasingly important by investors (Cohen and Simnett 2015). In the 2017 KPMG Survey of Corporate Social Responsibility Reporting, it is reported that 78% of G250 organizations now integrate financial and non-financial data in their annual reports, suggesting they believe CSR information is relevant for investors (KPMG 2017). However, whether the CSR disclosure is positively or negatively valued by investors is subject to contradictory findings (Cho, Michelon, Patten and Roberts 2015). This dissertation suggests that perhaps it is not the disclosure which holds the most significant weight, but the occurrence of CSR activities at all which contribute to the welfare of all economically linked individuals and organizations, including the subject organization itself.

CSR activity is observed directly through the voluntary disclosure or advertisement of organizations via a wide range of sources, including media releases, annual reports, web sites, and supplemental disclosures within the annual report (10-K) or standalone CSR reports. Initial studies find organizations who issue standalone CSR reports do so as a substantive signal of their superior commitment to CSR (Clarkson, Li, Richardson and Vasvari 2008). More recent studies expand upon such findings to show the U.S. organizations issuing standalone CSR reports are in fact better corporate citizens than organizations who do not issue standalone CSR reports (Mahoney, Thorne, Cecil and LaGore 2013), and also suggest the higher quality of the CSR report, the superior the CSR performance (Hummel and Schlick 2016). While disclosure of CSR activities and degree to which CSR activities are assured is worthy of future study, the prioritization and evidence of CSR activities is a measureable characteristic of IT Risk Culture. Although the association is supported by extant literature, research has yet to evaluate the association between the CSR activities and predominant risk response behavior reflective of the organization's IT Risk Culture.

2.7.3 IT Risk Culture Identification

Extant literature typically uses regression analysis to support associations between many of the IT Risk Culture elements and the likelihood of subsequent CSB. However, findings are oftentimes inconclusive and do not necessarily paint the full picture of comprehensive IT Risk Culture. When examining a complete sample with the use of regression analysis, the effects of each independent (i.e., classification) variable may cancel one another out (Stanley, Kellermanns and Zellweger 2017). Accounting researchers have been using cluster analysis since the 1970's with the goal of identifying organizations with similar characteristics and also to divide a given sample into meaningful subsamples so that items within a cluster are homogenous (Gupta and

Huefner 1972, Hoberg and Phillips 2010, Ding, Peng and Wang 2019). This dissertation seeks to do the same, as combined or synergistic effects of elements of an IT Risk Culture are able to differentially predict likelihood of subsequent CSBs.

A second limitation of variable centered techniques such as multivariate regression analysis is the assumption that independent variables have separate effects on the outcome variable. In line with the Theoretical Framework of ITG (**Figure 1)**, this dissertation specifically studies the three aspects of risk response; risk avoidance, risk reduction/mitigation and risk sharing/transfer. Therefore, in order to study the risk response function of IT Risk Culture and its association with subsequent CSB incident, a configural approach must be used to allow for consideration of risk response aspects as a system of interdependent variables. Utilizing a configural technique, notably cluster analysis, researchers can examine the effect that a pattern of variables have on an outcome. Most importantly, in contrast to variable centered techniques, configural approaches consider all variables jointly and explore the possibility that variables work together to influence outcomes. Clusters of organizations displaying similar patterns of variables are identified and compared to other clusters, in terms of patterns in the independent variables determining the clusters, and the outcomes associated with those clusters. Meaningful differences, evidenced by statistically unique clusters, emerge and allow for identification of differing types of IT Risk Culture.

Evidenced by the many control variables commonly utilized in regression analysis, there are many independent variables which may have a separate effect on prediction of CSB. However, in a cluster analysis it becomes problematic when the dimensionality in the analysis is too large (Bellman 1961). Therefore, in order to avoid this problem and to ensure adequate sample size, the select set of variables evidencing the risk response aspects of IT Risk Culture are utilized in this cluster analysis; cybersecurity disclosure sentiment, cybersecurity insurance, SOX-404 ICMW and CSR. Specifically, disclosure of sentiment represents a proxy measure for risk avoidance, SOX-404 and CSR represent proxy measures for risk mitigation/reduction and disclosure of cybersecurity insurance represents a proxy measure for risk sharing/transfer (**Figure 9**).

As an example of joint effects potentially caused by the identified independent variables, Cohen, Krishnamoorthy and Wright (2004) find the quality of general risk disclosures associated with the quality of corporate governance. Due to lack of a material financial consequence and unfavorable cost-benefit analysis, organizations lack incentive to operationalize environments which prevent cybersecurity breach. In contrast, CSR activities are associated with improvements in the quality and reliability of information. CSR activities are also the result of corporate governance, or in this instance IT Risk Culture, evidencing concern about economically linked individuals and organizations. As such, CSR activity should be not only be associated with higher quality cybersecurity risk disclosure, but more importantly strengthen the signal sent by the disclosure of the organization’s ability to prevent cybersecurity breach.

Furthermore, signaling theory assumes that it is less costly[1] for an organization with stronger performance to engage in disclosure than one with weaker performance (Verrecchia 1990). Within the context of cybersecurity, performance refers to stronger IT risk management than weaker IT risk management. As previously discussed, a synergistic IT Risk Culture is likely to negate cybersecurity instances due to the ability to identify specifically which IT vulnerabilities and risks are associated with the most damage to the organization. This identification is part of the continuous and holistic risk assessment completed by management

[1] Proprietary costs, such as preparation and competitive costs (Verrecchia, 1990).

and internal auditors exercising strong performing IT risk management. During this process the accuracy, design and operational execution of internal controls over financial reporting are monitored and assured by management annually per SOX-404 requirements. Synergistic effects of the variables representing IT Risk Culture should be considered, given this same IT risk management is responsible for the IT Risk Culture reflected in the cybersecurity risk disclosure and will evidence either a positive or negative sentiment related to risk, as well as the decision to insure against consequences of breach incidents based on their knowledge of internal control structure health. Accordingly, the effectiveness of an organization's internal control environment is intricately linked to the disclosure behavior of an organization and should jointly reflect an organization's ability to protect against cybersecurity incidents.

As the nature of the research question and purpose of the study should determine the approach, this study proposes the synergistic effects of different combinations of four variables evidencing IT Risk Culture (cybersecurity disclosure sentiment, disclosed cybersecurity insurance, SOX-404 ICMW and CSR) will combine to create distinct classifications or clusters, each uniquely predictive of CSB. Formal hypothesis to follow:

H3: Clusters of cybersecurity disclosure sentiment, disclosed cybersecurity insurance, SOX-404 material weakness, and corporate social responsibility will emerge and show meaningful differences reflective of IT Risk Culture and likelihood of subsequent cybersecurity breach.

The proposed models and hypotheses are included at **Figure 2, Figure 3** and **Table 3**, respectively.

Table 3: Summary of Hypotheses

Summary of Hypotheses

Hypothesis	Associations
H1a	The positive sentiment of cybersecurity risk disclosure is negatively associated with the likelihood of subsequently reported cybersecurity breach.
H1b	The negative sentiment of cybersecurity risk disclosure is positively associated with the likelihood of subsequently reported cybersecurity breach.
H2a	The presence of cybersecurity insurance coverage within the cybersecurity risk disclosure strengthens the negative association between positive disclosure sentiment and the likelihood of subsequently reported cybersecurity breach.
H2b	The presence of cybersecurity insurance coverage within the cybersecurity risk disclosure strengthens the positive association between negative disclosure sentiment and the likelihood of subsequently reported cybersecurity breach.
H3	Clusters of cybersecurity disclosure sentiment, disclosed cybersecurity insurance, SOX-404 material weakness, and corporate social responsibility will emerge and show meaningful differences reflective of IT Risk Culture and likelihood of subsequent cybersecurity breach.

Figure 2: Hypothesized Model 1

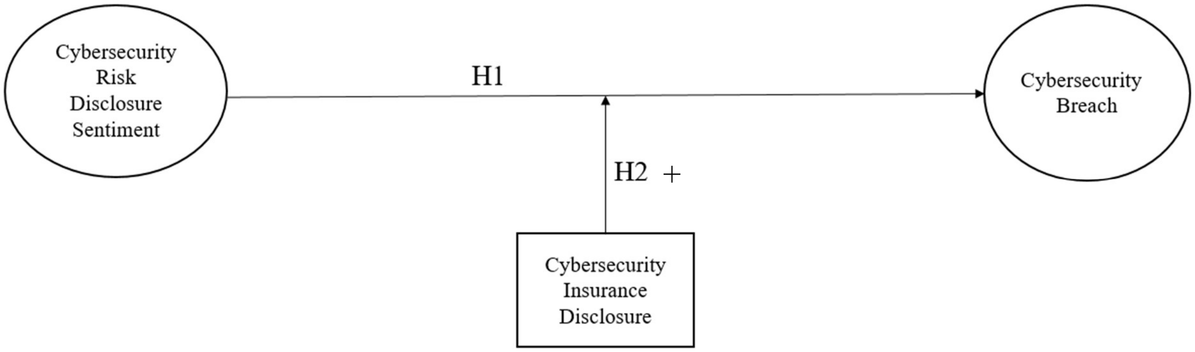
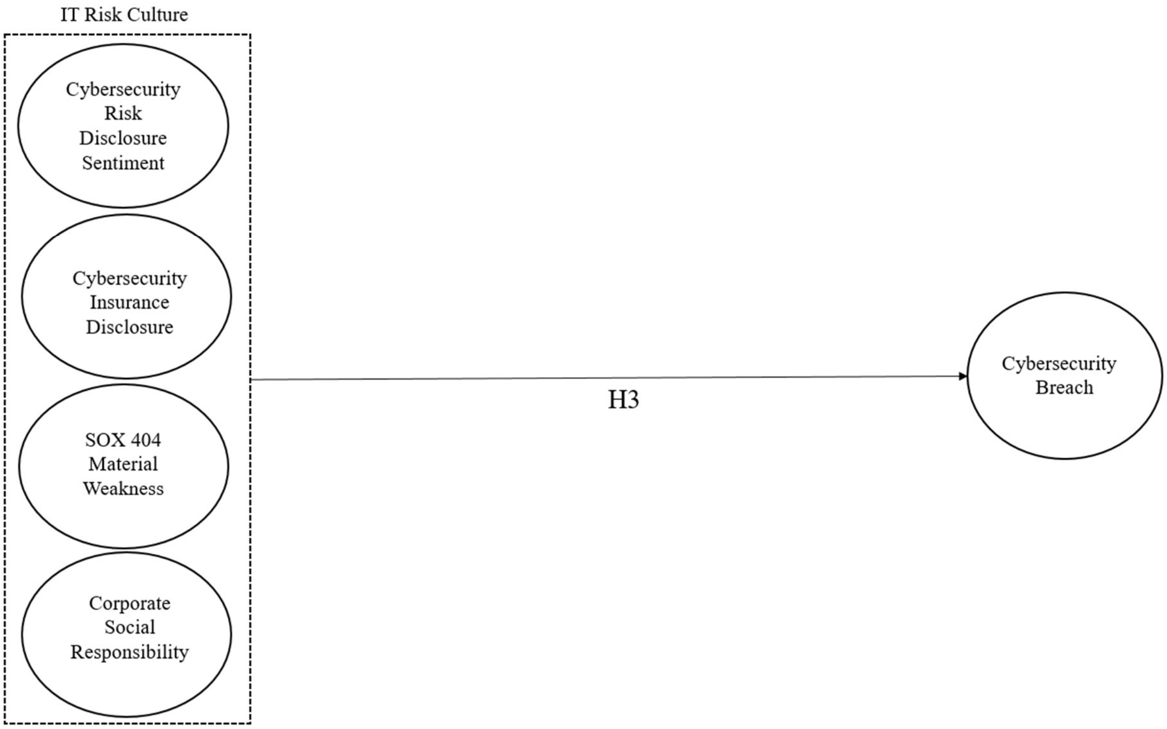

Cybersecurity Risk Disclosure Sentiment
H1
Cybersecurity Breach
H2 +
Cybersecurity Insurance Disclosure

Figure 3: Hypothesized Model 2


IT Risk Culture
Cybersecurity Risk Disclosure Sentiment
Cybersecurity Insurance Disclosure
SOX 404 Material Weakness
Corporate Social Responsibility
H3
Cybersecurity Breach

CHAPTER 3: METHODOLOGY

This chapter describes the sample, data collection procedures, measures and methodological techniques used to test the hypotheses.

3.1 Sample Selection

To analyze the association between cybersecurity risk disclosure content and related cybersecurity outcomes (i.e., CSB), capturing the impact of IT risk culture, I obtain organization data for S&P 1500 organizations from 2011 through 2019. I begin my investigation in 2011 which is the year in which the SEC first issued guidance on cybersecurity risk disclosure. Consistent with prior research, I exclude utility organizations (SIC codes 4900-4999) due to heightened regulation and abnormal disclosure policies in comparison to most other organizations (Karamanou and Vafeas 2005). The sample is limited to S&P 1500 organizations to allow for investigation of a variety of organizations from different industries and sizes.

The sample selection is reported in **Table 4**. I obtain 17,526 firm-year observations of cyber-related disclosure data from 2,071 unique organizations for the period 2011-2019. I exclude 1,308 unique organization year observations from the utilities industry and 2,997 observations with missing financial data. The final sample comprises 13,221 observations for 1,802 unique firms. I present the industry profile (by SIC code) of sample organizations in **Table 5**. About 93 percent of firms fall into four industry groups; manufacturing, wholesale trade and retail, financing and services. Approximately 98 percent of all recorded CSB also occur within the same four industry groups.

Table 4: Sample Selection

	Observations	Number of Firms
Sample Selection Procedure		
S&P 1500 firms (2011-2019)	17,526	2,071
Less observations:		
For utility firms	1,308	269
Missing financial data *	2,997	
Final valuation sample	**13,221**	**1,802**

This table presents the sample development process. The sample is based on S&P 1500 firms in the period 2011-2019.

* Other missing data includes missing Risk Item 1A Cybersecurity Risk Disclosure, CSR or other cluster variable data.

Table 5: Sample Industry Statistics

SIC Code	Industry Group	No. of Firms	%	No. of Subsequent Breach	%
0-999	Agriculture	5	0.3	3	0.9
1000-1999	Mining and Construction	122	6.8	3	0.9
2000-3999	Manufacturing	765	42.5	88	27.3
4000-4999	Transportation	1	0.1	0	-
5000-5999	Wholesale Trade and Retail	207	11.5	66	20.5
6000-6999	Financing Institutions	410	22.8	72	22.4
7000-8999	Services	288	16.0	90	28.0
9000-9999	Others	4	0.2	0	-
		1802	100	322	100

3.2 Measurement of Variables

Table 6 provides the definition, variable construction, and sources for all the variables used in this dissertation.

Table 6: Definitions for Variables

Dependent Variables			
Variable Name	**Sign**	**Variable Measurement**	**Source**
BREACH		An indicator variable indicating whether the organization incurred cybersecurity breach in year *t* + 1.	Privacy Rights Clearinghouse; Audit Analytics - Cybersecurity
Independent Variables			
NEG_TONE	+	The ratio of negative words to total words in the cyber extracts multiplied by 100 (based on Loughran and McDonald, 2011).	EDGAR
POS_TONE	(-)	The ratio of positive words to total words in the cyber extracts multiplied by 100 (based on Loughran and McDonald, 2011).	EDGAR
Moderating Variables			
CS_INS	+	An indicator variable for the disclosure of cybersecurity insurance at year *t*	EDGAR
Additional Variables			
ICMW		A count variable of internal control material weakness in year *t*	Audit Analytics
CSR		Combined ESG score	ASSET4 Thomson Reuters Datastream
Control Variables			
SIZE	+	Log of total assets at the beginning of the fiscal year	COMPUSTAT
AGE	+	Natural logarithm of the number of years since the organization's first appearance in COMPUSTAT	COMPUSTAT
GROWTH	+	One-year growth rate in sales in fiscal year *t*	COMPUSTAT
ROA	+	Net income divided by total assets	COMPUSTAT
LOSS	+	An indicator variable for loss year (net income < 0)	COMPUSTAT
LEVERAGE	+	Ratio of beginning total liabilities divided by beginning total assets in year *t*	COMPUSTAT
RETAIL	+	An indicator variable for the retail industry (SIC: 5000-5999)	COMPUSTAT

FINANCIAL	+	An indicator variable for the financial industry (SIC: 6000-6999)	COMPUSTAT
LENGTH	+	Total number of words in cybersecurity risk disclosure in fiscal year *t*, normalized by the average number of words in individual risk factor disclosed in Item 1A	EDGAR
10-K_LENGTH	+	The natural logarithm of the total number of words in the SEC Form 10-K filings	EDGAR
IT_ICMW	+	An indicator variable for presence of information technology internal control material weakness in year *t*	Audit Analytics
PAST_BREACH	+	An indicator variable for cybersecurity incident(s) in any year preceding fiscal year *t*	Privacy Rights Clearinghouse; Audit Analytics - Cybersecurity

3.2.1 Dependent Variable

The dependent variable (*BREACH*) is an indicator variable that denotes whether an organization experienced a cybersecurity incident in year *t* + 1, 0 otherwise. The year of cybersecurity incident is obtained from both the publicly held Privacy Rights Clearinghouse database (privacyrights.org) and privately held Audit Analytics – Cybersecurity database. Privacy Rights Clearinghouse publishes data breaches that primarily involve individual's identity while the Audit Analytics cybersecurity database collects all hacking incidents. Including both records of data breach ensure both internal and externally perpetrated breach incidents are included in variable measurement.

3.2.2 Independent Variables

The independent variables are obtained through textual analysis of cybersecurity risk disclosures included in the 10-K as reported in the SEC filings in the EDGAR system. According to Gao et al. (2020), cybersecurity risk disclosures are located in multiple sections of the annual report, however, 84.7% reside within Item 1A Risk disclosures. Therefore, to identify cybersecurity risk disclosures I first identify Item 1A within each 10-K using an approach similar to Campbell et al. (2014), Gaulin (2017), and Li et al. (2018). The SEC requires organizations include sub-captions summarizing the following risk to precede the full, related disclosure within Item 1A [2]. Using a bag of words approach, sub-captions related to cybersecurity risk disclosures are identified by observations of certain key words or phrases to denote risk factors related to cybersecurity. The key words or phrases were initially identified in prior research (Gordon et al., 2010; Li et al., 2018; Wang et al., 2013) and have been systematically updated per manual revision. **Appendix A** provides a list of these key words and phrases.

For each sub-caption found to be related to disclosure of cybersecurity risk, the sub-caption and paragraphs immediately following and up until the next sub-caption were extracted. Each sub-caption is assumed to represent a unique risk factor. I identify any and all related cybersecurity sub-captions and subsequent disclosure paragraphs from the Item 1A Risk Factors section of the 10-K. The combined text extraction is utilized to measure the following independent variables. For further description of textual analysis, see **Appendix B.**

Consistent with prior research, one independent variable of interest in the regression models is the disclosure tone (*NEG_TONE*) (*POS_TONE*) measured by the number of words that are negative (positive) divided by the total number of words in a given 10-K disclosure (Berkman et al. 2018). Negative (positive) tone will be captured using word lists from Loughran and McDonald (2011), which are restricted to words that have negative (positive) implications in a financial sense. A second independent variable (*CS_INS*) is an indicator variable for the disclosure of cybersecurity insurance at year *t* equal to 1 if disclosed in Item 1A cybersecurity risk disclosure, and 0 otherwise.

[2] Item 503(c) of Regulation S-K.

3.2.3 Cluster Variables

Internal control data is obtained from Audit Analytics. CSR data is obtained from the Thomson Reuters Datastream[3] database. Financial data is obtained from COMPUSTAT and EDGAR.

To test the impact of effective internal control system, I include internal control material weakness (*ICMW*), a count variable representing the pervasive nature of internal control material weakness reported during year *t* (Haislip, Masli et al. 2015, Han, Rezaee et al. 2015, Higgs, Pinsker et al. 2016). I also analyze a related variable, information technology internal control material weakness (*IT_ICMW*), a count variable representing the pervasive nature of information technology internal control material weakness reported during year *t*. Internal control data is obtained from the Audit Analytics database.

I obtain CSR scores from the Thomson Reuters ASSET4 database, now part of Refinitiv Datastream, which provides comprehensive CSR data for firms beginning in 2002 (Naughton et al. 2019). The combined CSR performance score (*CSR*) for an organization is based on a comprehensive evaluation of financial, governance, environmental and social dimensions.

3.2.4 Control Variables

I include control variables in my analyses to capture the effects of other determinants of cybersecurity breach incidents. The control variables are derived from prior literature to capture visibility, profitability, industry, and risk in the audit, accounting information systems and management information systems literatures. Since the control variables are discussed in detail in the relevant cited literature, I provide a brief discussion here.

[3] Proposal stated KLD database as source for CSR data, however, upon further review the data was limited to years 2011-2013 within the sample. In order to include CSR scores for all years within sample (2011-2019), the Thomson Reuters Datastream database was utilized, in accordance with extant literature (Naughton, Wang and Yeung et al. 2019) in which the attribute titled “Combined ESG Score” was identified for fiscal years 2011-2020.

The following control variables relate to the visibility of the organization (Li et al. 2018, Wang et al. 2013, Hilary et al. 2016). I control for size (*SIZE*) using total assets at year *t*. I also control for age (*AGE*) using the difference between year in sample and the year of the organization's first appearance in COMPUSTAT. Lastly, I control for growth (*GROWTH*) using the one-year growth rate in total revenue in fiscal year *t*.

The following control variables relate to the organization's financial condition. I control for profitability using a continuous measure (*ROA*) and an indicator (*LOSS*) for negative net income, where the variable is equal to 1 if net income is less than zero, and 0 otherwise. The (*LOSS*) control variable is relevant due to the likelihood of financially constrained organizations to not make sufficient investment in their internal controls over operations (Li, No et al. 2018). I also control for leverage (*LEVERAGE*) as this may cause differences in the relationships between CSR and other company measures (Mahoney et al. 2013). The variable is equal to the ratio of beginning total liabilities divided by beginning total assets in year *t*.

The following control variables relate to the organization's industry; given certain industries are at a higher propensity for cyberattacks than others. The two industries most commonly controlled for prior relevant studies are the retail and financial industries. These industries have been found to represent 2.3% and 1.8% of years observed exhibit data breaches (Ettredge et al. 2018). As such, (*RETAIL*) is an indicator variable used to control for organizations in the retail industry (SIC: 5000-5999) and is equal to 1 if the industry is retail, and 0 otherwise. (*FINANCIAL*) is also an indicator variable used to control for organizations in the financial industry (SIC: 6000-6999) and is equal to 1 if the industry is financial, and 0 otherwise.

The following control variables relate to other known predictors of cybersecurity risk. Prior studies find an association between length of cybersecurity risk disclosure and likelihood of future breach (Li et al. 2018). As such, I control for (*LENGTH*) which is measured as the total word count of total cybersecurity risk disclosure identified in Item 1A. Given that the *POS_TONE* and *NEG_TONE* metrics are based on key words found in form 10-K filings, I also control for the total number of words in the filings (*10-K_LENGTH*). To control for any previously experienced cybersecurity breach, going back to the first year of the sample (2011), I include an indicator variable (*PAST_BREACH*) equal to 1 if the organization experienced a breach incident at any point from 2005 until year *t*, and 0 otherwise.

3.3 Research Methods

3.3.1 Research Method - Model 1

Consistent with prior research employing a similar determinants model (Boritz & Timoshenko, 2015; Higgs et al., 2016), I employ probit models to examine the association between cybersecurity risk disclosure and subsequent CSB as proposed in Hypotheses 1a,b and 2a,b. This method is appropriate for dichotomous and continuous variables being examined in this study, including the multiple control variables that influence the main associations. Due to the binary nature of the dependent variable for hypotheses to be tested, the following probit regression models to test the general research design are formally:

$$\begin{aligned} BREACH = b_0 &+ b_1 NEG\_TONE + b_2 POS\_TONE \\ &+ b_3 SIZE + b_4 AGE + b_5 GROWTH + b_6 ROA + b_7 LOSS \\ &+ b_8 LEVERAGE + b_9 RETAIL + b_{10} FINANCIAL \\ &+ b_{11} LENGTH + b_{12} 10\text{-}K\_LENGTH + b_{13} PAST\_BREACH \\ &+ b_{14} IT\_ICMW + e \qquad (1) \end{aligned}$$

$$\begin{aligned} BREACH = b_0 &+ b_1 NEG\_TONE + b_2 POS\_TONE \\ &+ b_3 SIZE + b_4 AGE + b_5 GROWTH + b_6 ROA + b_7 LOSS \end{aligned}$$

$$\begin{aligned}
&+ b_{8}\mathit{LEVERAGE} + b_{9}\mathit{RETAIL} + b_{10}\mathit{FINANCIAL}\\
&+ b_{11}\mathit{LENGTH} + b_{12}\mathit{10\text{-}K\_LENGTH} + b_{13}\mathit{PAST\_BREACH}\\
&+ b_{14}\mathit{IT\_ICMW} + b_{15}\mathit{NEG\_TONE}{*}\mathit{CS\_INS}\\
&+ b_{16}\mathit{POS\_TONE}{*}\mathit{CS\_INS} + e
\end{aligned} \tag{2}$$

I winsorize all continuous variables at the 1st and 99th percentiles of their distributions to reduce the possibility that findings are driven by the presence of extreme outliers.

3.3.2 Research Method - Model 2

The second phase of the analysis is designed to test Hypotheses 3 and utilizes cluster analysis. While most variable-centered approaches (i.e., regression) examine variables in isolation, configural approaches such as cluster analysis allow researchers to examine the interdependencies among those variables (Stanley et al. 2017). Accounting research typically takes a variable centered approach with the goal of explaining as much variance as possible in a dependent variable, as utilized to test Hypotheses 1 and 2 in this dissertation. However, due to the limitation of variable-centered techniques having limited ability to detect complex interactions among multiple variables (Aguinis and Gottfredson 2010), scholars suggest the complimentary usage of configural approaches with other methodologies in order to obtain a more comprehensive view of how variables combine to influence outcomes (Zyphur 2009).

Accordingly, the third hypothesis aims to empirically identify meaningful differences in groupings amongst the five independent variables (e.g., cluster variables) identified using statistical cluster analysis. This methodology is of particular relevance to assessing Hypotheses 3 as cluster analysis is utilized to create groups (i.e., "clusters") of organizations which show similar patterns of outcomes representing various characteristics. Additionally, given this portion of the dissertation is designed from an inductive or exploratory approach, cluster analysis is an appropriate methodological tool (Ketchen and Shook 1996).

Statistical cluster analysis involves four steps: selection of classes or types of organizations; determination of measures of similarity between organization types; grouping of organizations into types; and the interpretation and description of results of grouping (Reid and Smith 2000). The types of organizations are determined per the sample selection process previously discussed. In determining measures of similarity between organization types, I rely on the theoretical framework of ITG (**Figure 1**). IT Risk Culture is determined by an organization's risk identification and risk response. H3 is designed to classify the risk response aspect of IT Risk Culture based on the following three behaviors: risk avoidance, risk reduction/mitigation and risk sharing/transfer.

Risk avoidance is hypothesized to be observed by sentiment expressed in cybersecurity risk disclosure. State previously in Chapter 2, the propensity of an organization to avoid risk is reflected by a negative sentiment, while proactive measures towards risk is reflected by a positive sentiment. The overall sentiment score is calculated by solving for the difference between the positive and negative sentiment scores calculated through textual analysis in accordance with the Loughran & McDonald (2011) dictionary. The cybersecurity risk disclosure sentiment cluster variable consists of integer values ranging between 75 and 3916, inclusive.

Risk reduction/mitigation is hypothesized to be reflected by two separate cluster variables; ICMW and CSR. As also discussed in Chapter 2, these measures are representative of an organization's care and concern for economically linked organizations through risk reduction and risk mitigation efforts observed by maintenance of effective internal control systems (*ICMW*) as well as care for all economically linked organizations and individuals (*CSR*). The

CSR score cluster variable consists of integer values ranging between 1.15 and 93.01, inclusive. The ICMW count cluster variable consists of integer values ranging between 0 and 14, inclusive.

Lastly, risk sharing/transfer is reflected by the final cluster variable, the disclosure of cybersecurity insurance. The disclosure of cybersecurity insurance is measured by the mention of any cybersecurity insurance policy within the Item 1A Risk Factor section of the 10-K. In this context, if a given organization discloses ownership of a cybersecurity insurance policy, then the cluster variable is assigned a value of 1. On the other hand, if a given organization does not disclose ownership of a cybersecurity insurance policy, the cluster variable is assigned a value of 0.

To account for variables not represented in standardized format, numeric attributes must be normalized to prevent the variable with the largest range from dictating outcomes. Accordingly, all cluster variables are normalized on a [0,1] scale (Al Shalabi et al., 2006). A second issue that must be addressed is the potential for correlation among predictor variables, resulting in endogeneity problems and suboptimal clustering results (Alawadhi & Byrnes, 2019). A common solution to this problem is principal components analysis which results in the calculation of a new set of variables from the original measures of similarity (Tan et al., 2016). The resulting cluster variables are linear combinations of the original dimensions which demonstrate zero correlation and can be used to complete effective cluster analysis and profiling (Byrnes, 2019).

After the necessary preprocessing of cluster variables, the appropriate clustering algorithm is determined. There are two partitioning procedures utilized in various clustering algorithms, hierarchical and nonhierarchical. In hierarchical cluster procedures the clustering algorithm solves for the identified number of clusters within the data, where as in nonhierarchical cluster procedures the analyst determines a pre-set number of clusters for the clustering algorithm to assign each data point (Hair, 2009). The preferred algorithm is most strongly dependent on the type of data being analyzed (Alpaydin, 2020), therefore the k-means non-hierarchical clustering algorithm is used to formulate an initial clustering prototype. The k-means algorithm partitions observations into a user-specified number of clusters and then iteratively reassigns observations until a numeric goal related to cluster distinctiveness is met (Hair, 2009). The default range for number of cluster iterations is set at 3 to 10, inclusive.

Utilizing a Euclidian metric, the k-means clustering algorithm calculates the dissimilarity between sets of attributes measured by the Euclidian squared distance. The technique minimizes within cluster variation, and maximizes between cluster variation in which case the distance between clusters is measured from respective centroids[4] (Reid and Smith 2000). In order to determine the best performing model in terms of cluster quality, I run the k-means algorithm three distinct times. The algorithm is set to identify 3, 4 and 5 clusters, respectively. I review the iteration history noting the change in cluster centers with each iteration, such that minimal change as of the final iteration is a determinant for accurate cluster assignment. To obtain a secondary confirmation of significant differences between cluster centroids, I utilize a one-way ANOVA and the Bonferroni Correction to test for significant differences between cluster variables by cluster. The cluster model with the most statistically significant differences between clusters is selected.

The principle components analysis of cluster variables will generate a scree plot, necessary for determining how many principle components identified are required to represent the majority of the cluster variables. A scatter plot of the identified representative principle

[4] The centroid is the point of means for a cluster. See Cooper and Weekers (1983).

components is generated, classified by cluster assignment. Normalized principal components are utilized in identifying meaningful differences between clusters. Descriptive statistics of cluster variable means within each identified cluster are interpreted to conclude differing IT Risk Culture – Risk Response profiles. Further analysis reveals the IT Risk Profiles' respective ability to differentially predict subsequent related outcomes, i.e., CSB.

CHAPTER 4: RESULTS

4.1 Descriptive Statistics

Table 7 presents descriptive statistics of the sample, comparing the split between *BREACH* firms and *NON-BREACH* firms. Panel A reports various univariate descriptive statistics for all variable in the complete sample. I report that 21.8 percent of my observations report *CS INS*, 11.4 percent of firm year observations have disclosed CSB in the past (*PAST_BREACH*), and 15 percent losses (*LOSS*).

Table 7: Descriptive Statistics

PANEL A

Descriptive Statistics for Variables in Equation (1) and (2)

		25th		75th	
(n = 13,221)	Mean	Percentile	Median	Percentile	Std. Dev.
BREACH	0.024	0.000	0.000	0.000	0.154
NEG_TONE	0.064	0.045	0.070	0.089	0.039
POS_TONE	0.006	0.000	0.005	0.009	0.007
CS_INS	0.218	0.000	0.000	0.000	0.413
SIZE	8.070	6.863	7.941	9.120	1.707
AGE	27.780	15.000	23.000	38.000	17.443
GROWTH	0.164	-0.008	0.060	0.147	5.397
ROA	0.039	0.011	0.041	0.079	0.123
LOSS	0.150	0.000	0.000	0.000	0.357
LEVERAGE	0.579	0.409	0.562	0.740	0.271
RETAIL	0.107	0.000	0.000	0.000	0.309
FINANCIAL	0.239	0.000	0.000	0.000	0.426
LENGTH	379.334	118.500	269.000	527.000	401.759
10-K_LENGTH	1176612	663707	948044	1394179	1037665
PAST_BREACH	0.114	0.000	0.000	0.000	0.107
IT_ICMW	0.012	0.000	0.000	0.000	0.318

Table 7: Descriptive Statistics (continued)

PANEL B

Descriptive Statistics: *BREACH* = 0 versus *BREACH* = 1

	BREACH = 0				*BREACH = 1*		
	(n = 12,899)				(n = 322)		
	Mean		Median	Std. Dev.	Mean	Median	Std. Dev.
NEG_TONE	0.0635		0.0699	0.0391	0.0654	0.0691	0.0324
POS_TONE	0.0063		0.0053	0.0068	0.0069	0.0060	0.0063
CS_INS	0.2151	***	0.0000	0.4109	0.3354	0.0000	0.4729
SIZE	8.0396	***	7.9175	1.6919	9.3064	9.1806	1.8575
AGE	27.7184	*	23.0000	17.4059	30.2205	26.0000	18.7192
GROWTH	0.1665		0.0602	5.4641	0.0798	0.0583	0.1557
ROA	0.0387	***	0.0406	0.1238	0.0596	0.0496	0.0698
LOSS	0.1507	**	0.0000	0.3578	0.1025	0.0000	0.3038
LEVERAGE	0.5764	***	0.5597	0.2674	0.6791	0.6374	0.3818
RETAIL	0.1046	***	0.0000	0.3060	0.2050	0.0000	0.4043
FINANCIAL	0.2396		0.0000	0.4269	0.2143	0.0000	0.4110
LENGTH	374.358	***	266.000	398.161	578.661	454.000	486.492
10-K_LENGTH	1172172	***	947526	1015612	1354478	979711	1693225
PAST_BREACH	0.1061	***	0.0000	0.3080	0.4441	0.0000	0.4976
IT_ICMW	0.0114	*	0.0000	0.1061	0.0217	0.0000	0.1461

*, **, *** Indicate the difference between the BREACH = 0 observations and the BREACH = 1 is significant at the 0.10, 0.05 and 0.01 levels, respectively, for the t-test of means.

The remaining Panel B in **Table 7** reports descriptive statistics for the full sample based on whether the organization reported CSB in year *t*+1. Inconsistent with expectations, there is no statistical significance between measures of *POS_TONE* or *NEG_TONE* in *BREACH* organizations. About 2.4 percent of organizations experience *BREACH* compared to 97.6 percent of organizations which do not experience *BREACH* during the sample period. Panel B reports that the 322 organizations reporting *BREACH* are more likely to disclose *CS_INS*.

Table 7 also shows means and medians for the control variables. Organizations with subsequent *BREACH* are more likely to have reported *PAST_BREACH*, more likely to experience *IT_ICMW* in year prior to breach, and more likely to have higher *LENGTH* of cybersecurity risk disclosure. Additionally, *BREACH* firms are on average larger and older, more likely to experience loss in year prior to CSB, and more likely to be in the retail industry. The overall results for the control variables are consistent with prior studies and thus confirm the need to include firm characteristics variables in the main analysis in order to capture incremental effect of independent variables on *BREACH*.

Pearson correlations for the *BREACH* variable are reported in **Table 8**. Consistent with prior research I report positive correlations among *BREACH* and *SIZE*, *AGE*, *ROA*, *LEVERAGE*, *RETAIL*, *LENGTH*, *10-K_LENGTH*, and *PAST_BREACH*. I also report negative correlations among *BREACH* and *LOSS*. Regarding H1, contrary to expectations, I report no correlation between *BREACH* and *POS_TONE* and *NEG_TONE*. Regarding H2, I report a significantly positive correlation between *BREACH* and *CS_INS*. Collectively, the descriptive analyses reported in Tables 7 and 8 provide univariate evidence suggesting organizations that disclose cybersecurity insurance report more breaches than organizations than firms who do not disclose cybersecurity insurance, while the role of sentiment expressed via cybersecurity risk disclosure remains unclear. To test for any instance of multicoliniarity, I review the standard errors and size of coefficients which show that they are not sensitive to the inclusion or exclusion of highly correlated variables (Hosmer and Lemeshow 1989), as well as review the VIF and tolerance measures which also confirm lack of multicoliniarity among variables.

Table 8: Pearson Correlations

Correlation Matrix: H1 and H2

(n = 13,221)

Variable	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
BREACH	.114**	.022*	(0.00)	.026**	-.021*	.058**	.050**	(0.01)	.078**	.027**	0.01	.164**	.045**	0.01	0.01
2. SIZE		.316**	-.034**	.049**	-.176**	.387**	-.065**	.318**	.147**	.433**	-.058**	.286**	.086**	.034**	.053**
3. AGE			-.023**	.055**	-.069**	.097**	0.00	-.151**	-.086**	.131**	(0.01)	.095**	-.060**	(0.01)	(0.01)
4. GROWTH				(0.01)	.023**	-.023**	(0.01)	(0.00)	(0.01)	(0.01)	(0.00)	(0.01)	(0.01)	(0.01)	(0.01)
5. ROA					-.505**	-.191**	.051**	-.050**	0.00	-.044**	-.027**	.046**	(0.02)	.023**	0.01
6. LOSS						.018*	-.029**	-.128**	(0.00)	-.040**	.032**	-.053**	0.00	-.030**	(0.01)
7. LEVERAGE							.067**	.260**	.090**	.215**	.032**	.167**	.069**	.041**	.061**
8. RETAIL								-.194**	0.01	-.130**	0.01	.119**	-.026**	.064**	0.01
9. FINANCIAL									.079**	.286**	-.036**	0.00	.135**	.026**	0.02
10. LENGTH										.089**	.019*	.239**	.451**	.198**	.207**
11. 10K_LENGTH											(0.01)	.093**	.054**	.032**	.035**
12. IT_ICMW												(0.01)	0.00	0.01	0.01
13. PAST_BREACH													.110**	.031**	.028**

14. CS_INS	**.077** **	**.140** **
15. POS_TONE		**.283** **
16. NEG_TONE		

The Pearson correlation coefficients are presented with the significant correlations in bold.

* correlation is significant at the 0.05 level (two-tailed); ** correlation is significant at the 0.01 level (two-tailed).

4.2 Model 1 – Probit Regression Results

Table 9 presents results of probit regressions combining *POS_TONE* and *NEG_TONE*, in addition to *CS_INS* and the control variables in the models. The inclusion of *CS_INS* improves the R^2 from 0.027 to 0.03. However, in column (1) I find that *POS_TONE* and *NEG_TONE* do not have statistically significant coefficients, suggesting that sentiment signaled regarding cybersecurity risk is not directly associated with subsequent breach. In column (2) I find that the moderating effect of *CS_INS* disclosure on *POS_TONE* and *NEG_TONE* also does not have statistically significant coefficients. This suggests that the disclosure of *CS_INS* does not strengthen the association between sentiment and subsequent breach. As a result, both H1 and H2 are not supported by this analysis. Interestingly, the regression results do however show statistically significant coefficients for *LENGTH* and *IT_ICMW,* suggesting these organization characteristics at year t are positively associated with likelihood of subsequent breach.

Table 9: Disclosure Sentiment and Disclosed Cybersecurity Insurance

	(1)		**(2)**		**(3)**		**(4)**	
	Coeff.	**p-value**	**Coeff.**	**p-value**	**Coeff.**	**p-value**	**Coeff.**	**p-value**
Intercept	-2.4497	0.0039	-2.3283	0.0061	-1.8675	0.0221	-2.1204	0.0113
POS_TONE	2.3948	0.6521	-0.2434	0.9688	2.665	0.7324	3.1731	0.5429
NEG_TONE	-1.1903	0.3834	-1.2010	0.3850	-1.8982	0.1686	-0.9316	0.4681
SIZE	0.1639	<.0001	0.1670	<.0001	0.1634	<.0001	0.1665	<.0001
AGE	-0.0041	0.0206	-0.0042	0.0191	-0.0039	0.0272	-0.00411	0.0209
GROWTH	-0.1277	0.3796	-0.1340	0.3609	-0.1368	0.3533	-0.1263	0.3912
ROA	1.5506	0.0023	1.5653	0.0021	1.5107	0.003	1.531	0.0026
LOSS	0.1136	0.3113	0.1179	0.2937	0.1112	0.3264	0.1118	0.3194
LEVERAGE	0.1741	0.2537	0.1705	0.2647	0.1624	0.2862	0.1639	0.2868
RETAIL	0.1583	0.0731	0.1669	0.0586	0.1792	0.0425	0.1785	0.0418
FINANCIAL	-0.1983	0.0129	-0.2226	0.0052	-0.2007	0.0119	-0.2098	0.0085
LENGTH	0.0903	0.0620	0.0665	0.1544	-0.0313	0.5396	0.0279	0.5600
10-K_LENGTH	-0.1140	0.0659	-0.1147	0.0682	-0.1119	0.0738	-0.1172	0.0618
PAST_BREACH	0.5226	<.0001	0.5154	<.0001	0.5015	<.0001	0.5096	<.0001
IT_ICMW	0.5337	0.0091	0.5444	0.0075	0.5243	0.01	0.5311	0.0089
*CS_INS*POS_TONE*			13.6007	0.2201				
*CS_INS*NEG_TONE*			0.1295	0.9229				
*LENGTH*POS_TONE*					0.0022	0.8694		
*LENGTH*NEG_TONE*					0.00458	0.019		
*CS_INS*LENGTH*							0.0002	0.0042
YEAR	Included		Included		Included		Included	
n	10,669		10,669		10,669		10,669	
R^2	0.027		0.03		0.0303		0.0304	
Correctly Classified	97.3		97.3		97.3		97.3	

One-tailed tests are shown for variables with a signed prediction. Two-tailed test are shown for variables with a signed prediction or when the coefficient sign is opposite the prediction.

All columns are from the probit regression equations (1) and (2). Dependent variable is *BREACH* (CSB at year *t* + 1).
POS_TONE was hypothesized to negatively predict breach; while *NEG_TONE* was hypothesized to positively predict breach. All variable definitions are included in **Table 6**.

4.3 Model 2 – Cluster Analysis Results

Table 10 shows the descriptive statistics for the five cluster variables per Hypotheses 3. Variables are normalized on a [0,1] scale. Initial cluster analysis is ran using the k-means algorithm with the default range for the number of cluster iterations set at 3 to 10, inclusive. Results of k-means algorithm cluster iterations at preset number of clusters 3, 4 and 5 are displayed in **Table 11**. I observe the 3 cluster model is the most stable model as of the 10th iteration. Cluster assignments are made based on the 3 cluster model and a preliminary scatterplot is utilized to visualize the distinct differences in clusters (**Figure 4**).

Table 10: Descriptive Statistics for Cluster Variables

(n = 6817)	Mean	Minimum	Maximum	Std. Dev.
CS_INS	0.286	0.000	1.000	0.452
POS_TONE	0.008	0.000	0.060	0.006
NEG_TONE	0.078	0.000	0.194	0.024
ICMW	0.063	0.000	14.000	0.464
CSR	41.982	1.152	93.015	17.370

Table 11: Iteration History for Cluster Models

3 Clusters:

Iteration History			
	Change in Cluster Centers		
Iteration	1	2	3
1	0.000	8.798	6.566
2	5.415	0.012	0.709
3	4.898	0.020	1.418
4	1.139	0.002	0.097
5	3.642	0.000	0.525
6	1.887	0.000	0.501
7	0.000	0.000	0.000

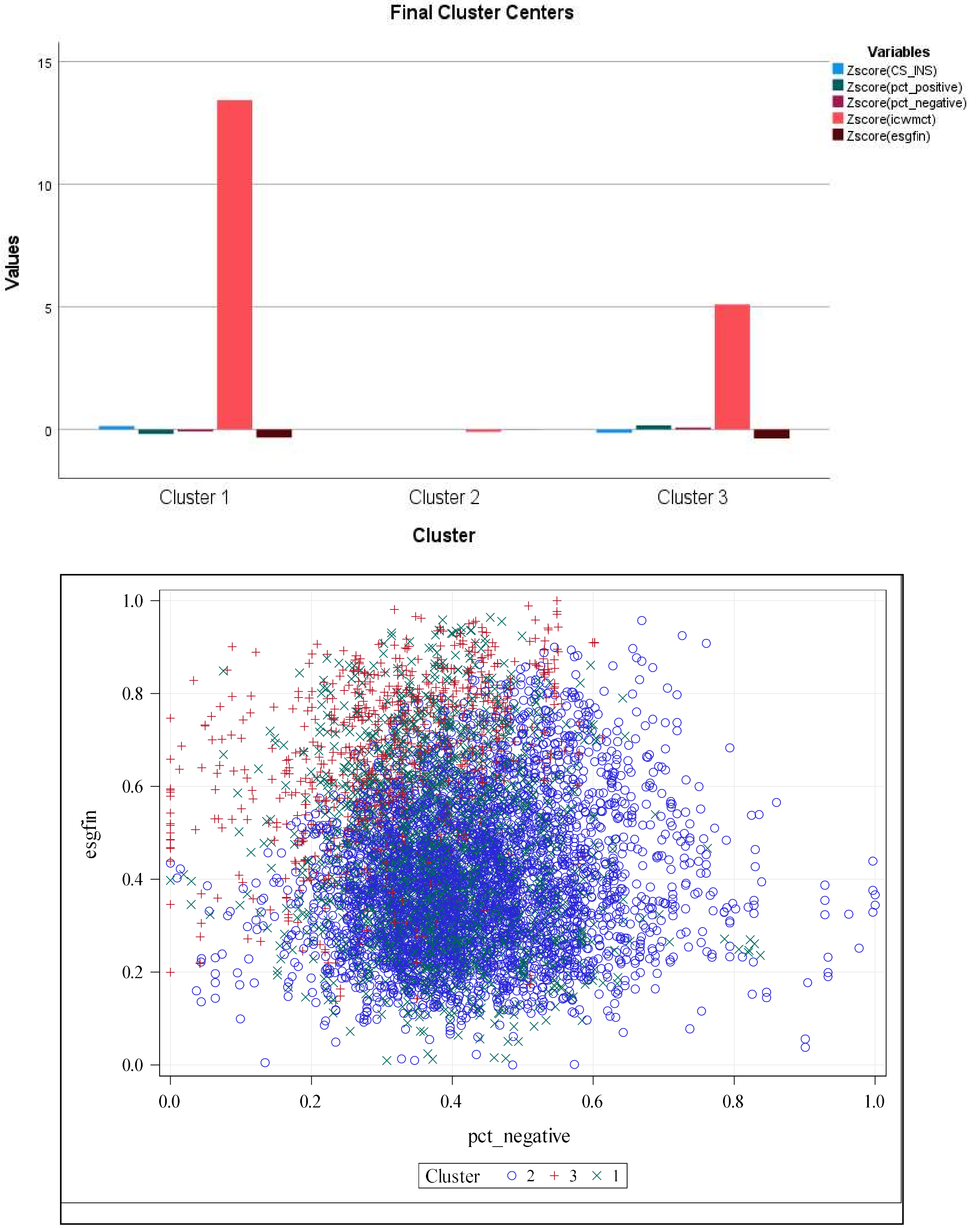
4 Clusters:

Iteration History				
	Change in Cluster Centers			
Iteration	1	2	3	4
1	0.000	2.374	4.305	3.722
2	0.000	0.070	1.272	0.000
3	0.000	0.072	0.711	0.000
4	0.000	0.071	0.455	0.000
5	0.000	0.061	0.286	0.000
6	0.000	0.040	0.163	0.000
7	0.000	0.034	0.129	0.000
8	0.000	0.033	0.111	0.000
9	0.000	0.035	0.105	0.000
10	0.000	0.040	0.109	0.000

5 Clusters:

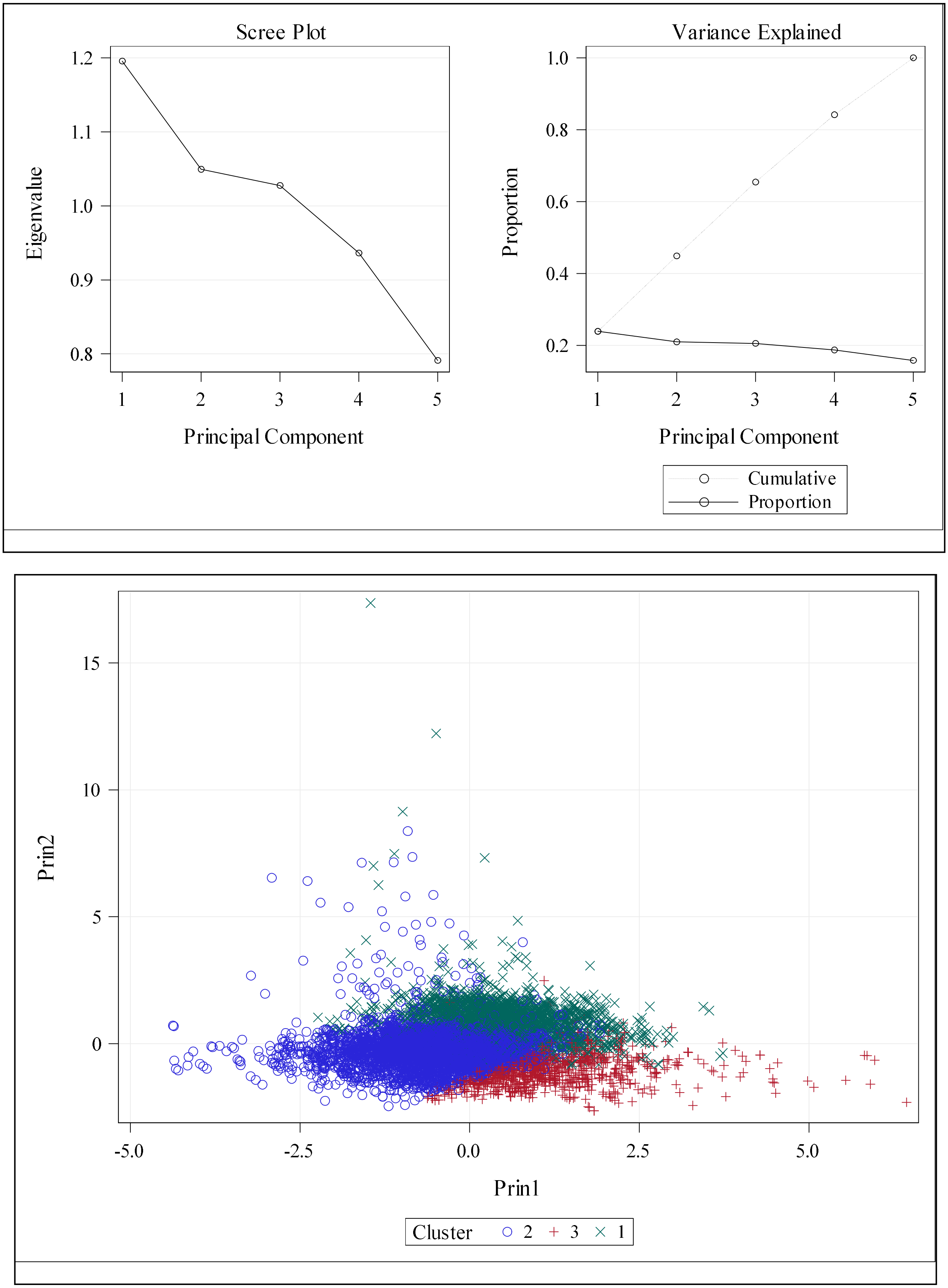
Iteration History					
	Change in Cluster Centers				
Iteration	1	2	3	4	5
1	0.000	4.345	4.903	3.066	5.534
2	0.000	2.105	0.079	2.915	0.735
3	0.000	0.524	0.069	1.430	0.449
4	0.000	0.000	0.064	0.000	0.298
5	0.000	0.000	0.041	0.000	0.164
6	0.000	0.000	0.034	0.000	0.127
7	0.000	0.000	0.033	0.000	0.112
8	0.000	0.000	0.037	0.000	0.109
9	0.000	0.000	0.040	0.000	0.108
10	0.000	0.000	0.038	0.000	0.094

Figure 4: Initial Cluster Model Bar Chart and Scatter Plot



Bar and scatter charts (**Figure 4**) are utilized to demonstrate differences in clusters by cluster variable means, although results are not clear due to the correlation among predictor variables. As such, a principle components analysis is completed and results of the scree plot and related graph showing what proportion of variance is explained by each principal component are included at **Figure 5**. Following the dotted line in **Figure 5**, the cumulative proportion of variance explained by the first two principal components is 44 percent.

Figure 5: Principal Components Analysis



A second scatterplot is generated using the two largest principle components (**Figure 5**) and three clusters are apparent. As a final step in cluster analysis, a one-way ANOVA is generated for each of the 5 cluster variables classified by the three identified clusters (**Table 12**). While some statistical significance is noted between means of clusters for cluster variables ICMW and CSR, the majority of mean cluster variables are not statistically different between clusters. As a final step, the clusters are regressed on *BREACH* variable, with the five cluster variables held constant, and no significant likelihood of subsequent CSB is observed (**Table 13**). As such, H3 is found null as no significant differences of cluster variable means are found within clusters. Accordingly, no statistically significant IT Risk Profiles are identified or associated with future subsequent breach using the cluster variables originally hypothesized at H3.

Table 12: Statistical Difference of Cluster Means

						95% Confidence Interval	
Dependent Variable			Mean Difference	Std. Error	Sig.	Lower Bound	Upper Bound
CS_INS	1	2	0.140	0.224	1.000	-0.396	0.676
		3	0.283	0.250	0.773	-0.315	0.881
	2	1	-0.140	0.224	1.000	-0.676	0.396
		3	0.143	0.112	0.604	-0.125	0.410
	3	1	-0.283	0.250	0.773	-0.881	0.315
		2	-0.143	0.112	0.604	-0.410	0.125
POS_TONE	1	2	-0.187	0.224	1.000	-0.723	0.349
		3	-0.361	0.250	0.445	-0.959	0.237
	2	1	0.187	0.224	1.000	-0.349	0.723
		3	-0.174	0.112	0.361	-0.441	0.094
	3	1	0.361	0.250	0.445	-0.237	0.959
		2	0.174	0.112	0.361	-0.094	0.441
NEG_TONE	1	2	-0.087	0.224	1.000	-0.623	0.450
		3	-0.169	0.250	1.000	-0.767	0.429
	2	1	0.087	0.224	1.000	-0.450	0.623
		3	-0.082	0.112	1.000	-0.350	0.186
	3	1	0.169	0.250	1.000	-0.429	0.767
		2	0.082	0.112	1.000	-0.186	0.350
ICMW	1	2	13.53236135*	0.087	0.000	13.324	13.741
		3	8.32948947*	0.097	0.000	8.097	8.562
	2	1	-13.53236135*	0.087	0.000	-13.741	-13.324
		3	-5.20287187*	0.043	0.000	-5.307	-5.099
	3	1	-8.32948947*	0.097	0.000	-8.562	-8.097
		2	5.20287187*	0.043	0.000	5.099	5.307
CSR	1	2	-0.341	0.224	0.382	-0.877	0.195
		3	0.033	0.249	1.000	-0.564	0.631
	2	1	0.341	0.224	0.382	-0.195	0.877
		3	.37440695*	0.112	0.002	0.107	0.642
	3	1	-0.033	0.249	1.000	-0.631	0.564
		2	-.37440695*	0.112	0.002	-0.642	-0.107

*. The mean difference is significant at the 0.05 level.

Table 13: IT Risk Profile and Cybersecurity Breach

Analysis of Maximum Likelihood Estimates						
Parameter		**DF**	**Estimate**	**Standard Error**	**Wald Chi-Square**	**Pr > ChiSq**
Intercept		1	-1.8066	0.1758	105.5745	<.0001
CLUSTER	**1**	1	0.1552	0.1031	2.2633	0.1325
CLUSTER	**2**	1	-0.0942	0.11	0.7337	0.3917
CLUSTER	**3**	0	0	.	.	.
CS_INS		0	0	.	.	.
POS_TONE		1	-0.0447	0.3151	0.0201	0.8873
NEG_TONE		1	-0.4375	0.2539	2.9694	0.0849
ICMW		1	-0.6568	1.099	0.3571	0.5501
CSR		1	0.3741	0.1726	4.6955	0.0302

Variable descriptions included on **Table 6**. Dependent variable is *BREACH* (CSB at year *t* + 1).

4.4 Supplemental Analyses

4.4.1 Supplemental Analyses – Model 1

While the hypothesized associations were not found statistically significant, another key attribute of the cybersecurity risk disclosure, *LENGTH*, was found statistically significant in model (1). As such, in model (3) in **Table 9** I review the moderating effect of *LENGTH* on the ability of sentiment to predict subsequent breach, noting statistically significant coefficient on the interaction effect between *NEG_TONE* and *LENGTH*. I consider this finding very interesting since it indicates that, although there is no main effect of sentiment on future breach likelihood, when negative sentiment is expressed within a lengthy cybersecurity risk disclosure, there is positive significant likelihood of subsequent breach.

Additionally, while the hypothesized moderating effect of *CS_INS* on *POS_TONE* and *NEG_TONE* was found not significant, I review the moderating effect of *CS_INS* on *LENGTH* in model (4) in **Table 9**. I find this interaction effect both positive and significant, indicating the disclosure of *CS_INS* within a lengthy cybersecurity risk disclosure to be positively associated with likelihood of subsequent breach. While not included as an independent variable in **Table 9**, in a supplemental analysis I review the direct association between *CS_INS* and *BREACH*, noting positive coefficient with insignificant p-value (0.064). Additionally, with each of the models (3) and (4) the R^2 increases above hypothesized models.

4.4.2 Supplemental Analysis – Model 2

CSR as an organizational characteristic is not introduced as a component of IT Risk Culture until the third hypothesis. However, as there is no extant literature which examines the direct association between CSR activity and subsequent CSB, the following probit regression is utilized:

$$\begin{aligned} BREACH = {} & b_0 + b_1 CSR \\ & + b_2 SIZE + b_3 AGE + b_4 GROWTH + b_5 ROA + b_6 LOSS \\ & + b_7 LEVERAGE + b_8 RETAIL + b_9 FINANCIAL \\ & + b_{10} LENGTH + b_{11} 10\text{-}K\_LENGTH + b_{12} PAST\_BREACH \\ & + b_{13} IT\_ICMW + e \end{aligned} \tag{3}$$

Table 14 presents results of probit regressions combining CSR and firm characteristics, along with other cluster variables, in the models. In model (1) I find that organization CSR activity does not have a statistically significant coefficient, suggesting that CSR activity does not have a main effect on predicting the likelihood of subsequent CSB. To test for any instance of multicoliniarity, I review correlation coefficients, VIF and tolerance measures which confirm lack of multicoliniarity among variables in Equation (3).

Table 14: Corporate Social Responsibility and Cybersecurity Breach

	(1)		(2)		(3)	
	Coeff.	**p-value**	**Coeff.**	**p-value**	**Coeff.**	**p-value**
Intercept	-2.482	0.009	-2.317	0.015	-2.313	0.016
CSR	-0.001	0.493	-0.003	0.234	-0.002	0.590
SIZE	0.180	<.0001	0.180	<.0001	0.186	<.0001
AGE	-0.005	0.009	-0.005	0.008	-0.005	0.009
GROWTH	-0.129	0.440	-0.127	0.453	-0.125	0.463
ROA	1.537	0.010	1.510	0.011	1.540	0.011
LOSS	0.180	0.161	0.182	0.155	0.182	0.158
LEVERAGE	0.002	0.991	-0.001	0.997	0.008	0.961
RETAIL	0.177	0.100	0.187	0.083	0.172	0.120
FINANCIAL	-0.146	0.090	-0.170	0.047	-0.162	0.060
LENGTH	0.077	0.149	0.046	0.355	0.065	0.227
10-K_LENGTH	-0.106	0.131	-0.104	0.148	-0.115	0.103
PAST_BREACH	0.512	<.0001	0.512	<.0001	0.513	<.0001
IT_ICMW	0.377	0.193	0.391	0.173	0.362	0.217
*CS_INS*CSR*			0.004	0.012		
*POS_TONE*CSR*					0.234	0.051
*NEG_TONE*CSR*					-0.028	0.383
YEAR	Included		Included		Included	
n	6,918		6,918		6,918	
R^2	0.032		0.033		0.0331	
Correctly Classified	96.5		96.5		96.5	

One-tailed tests are shown for variables with a signed prediction. Two-tailed test are shown for variables with a signed prediction or when the coefficient sign is opposite the prediction.
Variable descriptions included on **Table 6**. All columns are from the probit regression equation (3). Dependent variable is *BREACH* (CSB at year *t* + 1).

In model (2) and model (3) of **Table 14** I review for moderating effects of *CS_INS*, in addition to both *POS_TONE* and *NEG_TONE*, on the main association between CSR and subsequent breach. In model (2) I find that the moderating effect of *CS_INS* on *CSR* does have a statistically significant coefficient, suggesting that CSR activity for a firm disclosing *CS_INS* does predict the likelihood of subsequent CSB. Additionally, in model (3) I find no statistically significant coefficient on the moderating effect of *NEG_TONE* and *CSR*, however, I do find a moderately significant coefficient on the moderating effect of *POS_TONE* and *CSR*. Results of this combined regression suggest that CSR activity is likely a factor in holistic IT risk response.

In response to these supplemental analyses regarding the direct association between CSR activity and the likelihood of subsequent breach, I revisit the cluster analysis (H3). This cluster analysis is by definition an exploratory analysis designed to identify IT Risk Profiles related to IT Risk Culture - Risk Response behavior (**Figure 1**). In this study, I measure organizational IT Risk Culture – Risk Response by disclosed behavior. These behaviors are disclosed and measured by primarily the Item 1A Risk Factor cybersecurity risk disclosure components (i.e., sentiment, length, disclosure of cybersecurity insurance) but also disclosed CSR activity. As such, it is logical that the *ICMW* variable was not found a significant cluster variable in the testing of H3. While IT internal control effectiveness is associated with subsequent breach (**Table 9**), it is disclosed to the public in a matter of compliance in accordance with SOX-404 guidelines, not specifically related to signaling of IT Risk Culture – Risk Response. Furthermore, as a result of analysis at **Table 9**, it is evident that cybersecurity disclosure length is a key component in the signaled IT Risk Culture – Risk Response. Accordingly, a supplemental cluster analysis is completed with the following five cluster variables; *LENGTH, POS_TONE, NEG_TONE, CS_DIS* and *CSR*.

Table 15 shows the descriptive statistics for the five revised cluster variables. Variables are normalized on a [0,1] scale. Initial cluster analysis is ran using the k-means algorithm with the default range for the number of cluster iterations set at 3 to 10, inclusive. Results of k-means algorithm cluster iterations at preset number of clusters 3, 4 and 5 are displayed in **Table 16**. Once again, I observe the 3 cluster model is the most stable model as of the 10th iteration. Cluster assignments are made based on the 3 cluster model and a preliminary scatterplot is utilized to visualize the distinct differences in clusters (**Figure 6**).

Table 15: Descriptive Statistics for Second Cluster Analysis

(n = 6817)	Mean	Minimum	Maximum	Std. Dev.
CS_INS	0.286	0.000	1.000	0.452
POS_TONE	0.008	0.000	0.060	0.006
NEG_TONE	0.078	0.000	0.194	0.024
LENGTH	518.246	75.000	6435.000	419.503
CSR	41.982	1.152	93.015	17.370

Table 16: Iteration History for Cluster Models in Second Cluster Analysis

3 Clusters:

Iteration History

	Change in Cluster Centers		
Iteration	1	2	3
1	10.454	10.607	10.465
2	0.166	1.447	0.158
3	0.116	0.848	0.251
4	0.121	0.638	0.366
5	0.240	0.446	0.281
6	0.299	0.313	0.371
7	0.214	0.144	0.524
8	0.076	0.075	0.257
9	0.021	0.024	0.071
10	0.010	0.007	0.035

4 Clusters:

Iteration History

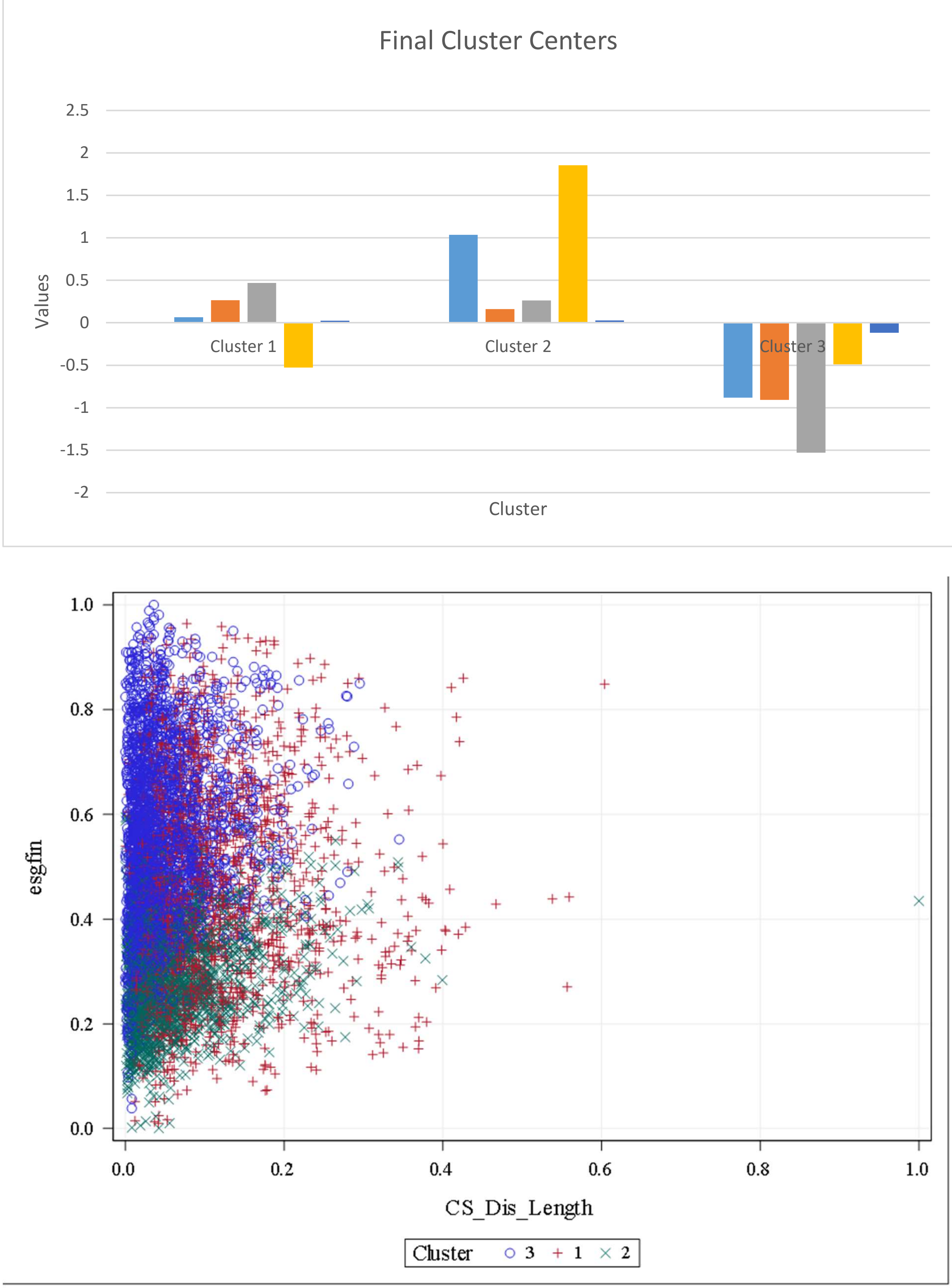
	Change in Cluster Centers			
Iteration	1	2	3	4
1	0.000	0.000	4.656	3.760
2	0.000	5.465	1.831	0.029
3	0.000	4.026	1.146	0.054
4	0.000	2.070	0.628	0.095
5	0.000	1.132	0.480	0.149
6	0.000	0.701	0.266	0.165
7	0.000	0.598	0.199	0.214
8	0.000	0.469	0.228	0.220
9	0.000	0.141	0.230	0.078
10	0.000	0.055	0.210	0.099

5 Clusters:

Iteration History

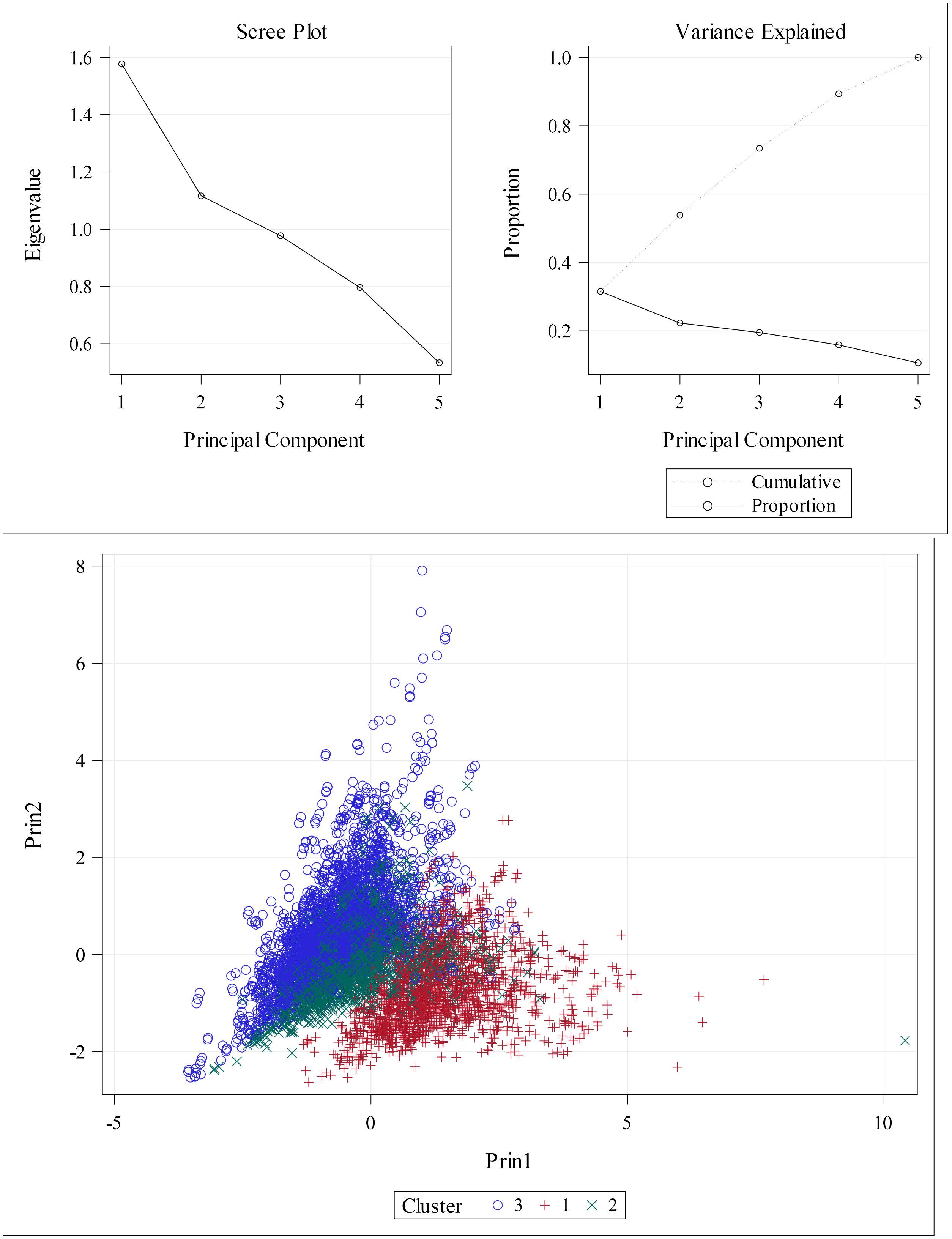
	Change in Cluster Centers				
Iteration	1	2	3	4	5
1	0.000	2.978	4.296	3.658	0.000
2	0.000	0.165	1.863	0.735	0.000
3	3.553	0.209	1.253	0.583	0.000
4	2.705	0.193	0.689	0.416	0.000
5	2.939	0.062	0.462	0.126	0.000
6	1.724	0.059	0.316	0.149	0.000
7	1.064	0.054	0.241	0.182	0.000
8	0.582	0.074	0.202	0.111	0.000
9	0.311	0.087	0.198	0.074	0.000
10	0.183	0.104	0.195	0.045	0.000

Figure 6: Initial Cluster Model Bar Chart and Scatter Plot for Second Cluster Analysis



Bar and scatter charts (**Figure 6**) demonstrate differences in clusters by cluster variable means. While it is evident from the bar chart that clusters do have significant differences in means of cluster variables, unlike the equivalent chart from the initial cluster analysis (**Figure 4**), the scatterplot does reflect ambiguity due to the correlation among predictor variables. In response, a principle components analysis is completed and results of the scree plot and related graph showing what proportion of variance is explained by each principal component are included at **Figure 7**. Following the dotted line in **Figure 7**, the cumulative proportion of variance explained by the first two principal components is nearly 60 percent, which is much higher than the PCA results from the initial cluster analysis (H3).

Figure 7: Principal Components Analysis for Second Cluster Analysis



A second scatterplot is generated using the two largest principle components (**Figure 7**) and three clusters are again apparent. As a final step in cluster analysis, a one-way ANOVA is generated for each of the 5 cluster variables classified by the three identified clusters (**Table 17**). I report statistical significance between the means of all 5 cluster variables within each of the three identified clusters, with the exception of no statistical difference noted in CSR activity scores between cluster 1 and 2. As a final step, the clusters are regressed on the BREACH variable (**Table 18**), with the five cluster variables held constant, and I report statistically significant coefficient for the association between Cluster 1 and the positive likelihood of subsequent breach.

Table 17: Statistical Difference of Cluster Means for Second Cluster Analysis

						95% Confidence Interval	
Dependent Variable			Mean Difference	Std. Error	Sig.	Lower Bound	Upper Bound
LENGTH	1	2	-389.758*	9.359	0.000	-412.17	-367.35
		3	381.111*	10.715	0.000	355.45	406.77
	2	1	389.758*	9.359	0.000	367.35	412.17
		3	770.869*	12.279	0.000	741.47	800.27
	3	1	-381.111*	10.715	0.000	-406.77	-355.45
		2	-770.869*	12.279	0.000	-800.27	-741.47
CS_INS	1	2	-.984*	0.002	0.000	-0.99	-0.98
		3	-.015*	0.002	0.000	-0.02	-0.01
	2	1	.984*	0.002	0.000	0.98	0.99
		3	.969*	0.003	0.000	0.96	0.98
	3	1	.015*	0.002	0.000	0.01	0.02
		2	-.969*	0.003	0.000	-0.98	-0.96
POS_TONE	1	2	.00070923462226*	0.000	0.000	0.000	0.001
		3	.00793098402747*	0.000	0.000	0.008	0.008
	2	1	-.00070923462226*	0.000	0.000	-0.001	0.000
		3	.00722174940521*	0.000	0.000	0.007	0.008
	3	1	-.00793098402747*	0.000	0.000	-0.008	-0.008
		2	-.00722174940521*	0.000	0.000	-0.008	-0.007
NEG_TONE	1	2	.0080618039444*	0.001	0.000	0.007	0.010
		3	.0778360500154*	0.001	0.000	0.076	0.079
	2	1	-.0080618039444*	0.001	0.000	-0.010	-0.007
		3	.0697742460709*	0.001	0.000	0.068	0.072
	3	1	-.0778360500154*	0.001	0.000	-0.079	-0.076
		2	-.0697742460709*	0.001	0.000	-0.072	-0.068
CSR	1	2	-0.058949723645320	0.469	1.000	-1.182	1.064
		3	2.495948943116211*	0.537	0.000	1.210	3.782
	2	1	0.058949723645320	0.469	1.000	-1.064	1.182
		3	2.554898666761531*	0.615	0.000	1.081	4.029
	3	1	-2.495948943116211*	0.537	0.000	-3.782	-1.210
		2	-2.554898666761531*	0.615	0.000	-4.029	-1.081

*. The mean difference is significant at the 0.05 level.

Table 18: IT Risk Profile and Cybersecurity Breach for Second Cluster Analysis

	Coeff.	**p-value**
Intercept	2.319	<.0001
CLUSTER 1	0.184	0.018
CLUSTER 2	0.143	0.145
CLUSTER 3	0.000	.
LENGTH	1.696	<.0001
CS_INS	0.000	.
POS_TONE	0.264	0.395
NEG_TONE	0.060	0.828
CSR	0.573	0.002
n	6,817	

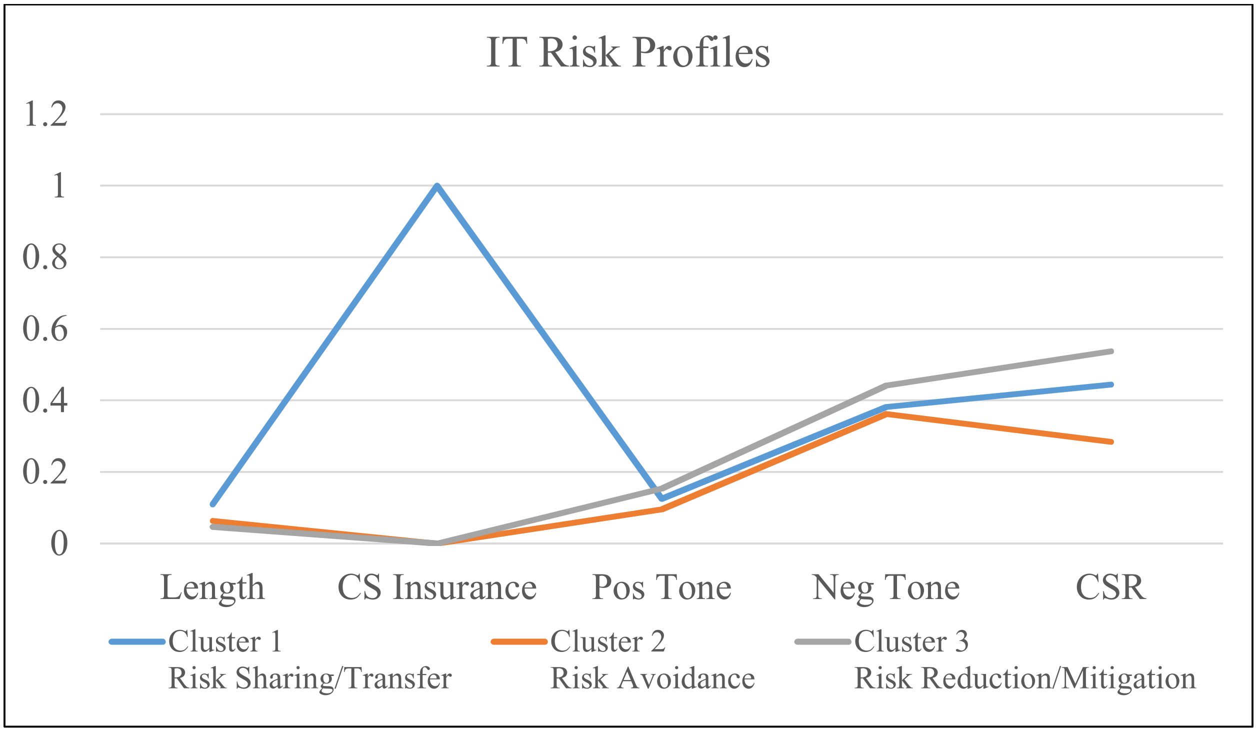
Variable descriptions included on **Table 6**. Dependent variable is *BREACH* (CSB at year *t* + 1).

Table 19 presents the descriptive statistics for each of the five cluster variables grouped by cluster while **Figure 8** provides a visualization of cluster differentiation. Cluster 1, the only cluster representative of organizations likely to experience subsequent breach, contains the longest cybersecurity risk disclosures and is the only cluster to disclose cybersecurity insurance. Cluster 2 contains the lowest CSR score as well as the lowest positive sentiment measure. Cluster 3 contains the highest CSR score as well as the highest positive sentiment measure. Negative sentiment is highest in cluster 3 and lowest in cluster 2, but the average score is similar enough to suggest boiler plate disclosure language of predominant negative sentiment.

Table 19: Descriptive Statistics by IT Risk Culture – Risk Response

	N	Mean	Minimum	Maximum	Std. Dev.
(1) Risk Sharing/Transfer	1951				
LENGTH		0.110	0.000	0.604	0.080
CS_INS		1.000	1.000	1.000	0.000
POS_TONE		0.125	0.000	0.479	0.079
NEG_TONE		0.382	0.000	0.837	0.100
CSR		0.445	0.010	0.964	0.189
(2) Risk Avoidant	1810				
LENGTH		0.064	0.000	1.000	0.062
CS_INS		0.000	0.000	0.000	0.000
POS_TONE		0.096	0.000	0.479	0.077
NEG_TONE		0.362	0.000	0.846	0.114
CSR		0.285	0.000	0.687	0.096
(3) Risk Reduction/Mitigation	3056				
LENGTH		0.047	0.000	0.345	0.043
CS_INS		0.000	0.000	0.000	0.000
POS_TONE		0.154	0.000	1.000	0.120
NEG_TONE		0.442	0.000	1.000	0.136
CSR		0.538	0.038	1.000	0.167

Figure 8: Visualization of Cluster Membership by Cluster Variable



According to this analysis of cluster variables within each identified cluster, the IT Risk Culture of an organization can be profiled by observing one predominant Risk Response behavior (**Figure 8**). In accordance with the theoretical framework of IT Governance (**Figure 1**), cluster 1 represents the Risk Sharing/Transfer predominant IT Risk Culture. These organizations represent the only IT Risk profile statistically likely to experience future (disclosed) CSB. Cluster 2 represents the Risk Avoidant predominant IT Risk Culture. As the IT Risk profile expressing the least positive and least negative sentiment, lowest CSR activity, shorter length cybersecurity risk disclosure, and lack of cybersecurity insurance, the collective sum of disclosed behaviors is minimal. Cluster 3 represents the Risk Reduction/Mitigation predominant IT Risk Culture. While the shortest in cybersecurity risk disclosure length and not likely to disclose cybersecurity insurance, organizations within this IT Risk profile contain the highest CSR scores, along with the highest positive and negative sentiment expressed within disclosure.

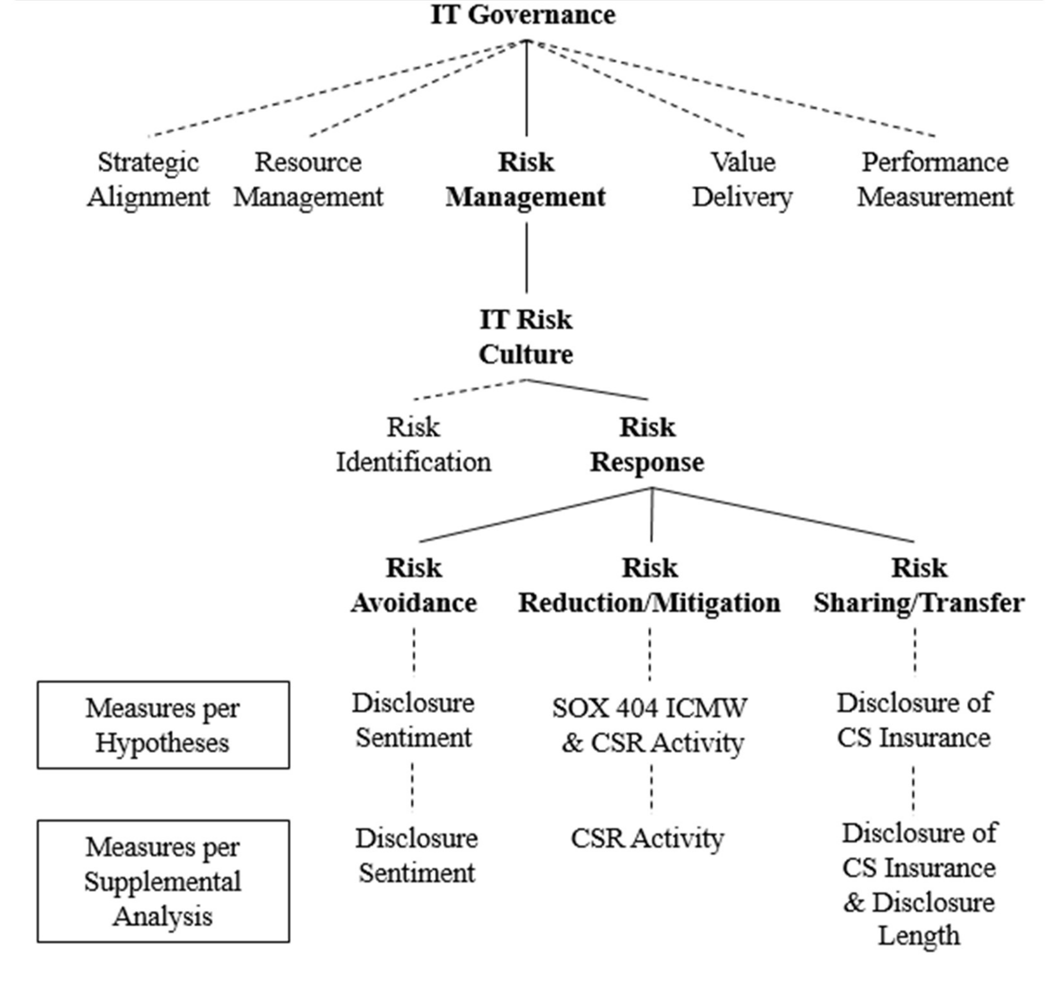
CHAPTER 5: DISCUSSION

5.1 Theoretical Contributions

I first investigate the association between cybersecurity risk disclosure content and subsequent CSB. I specifically study the signal sent by the contents of the disclosure, focusing on the disclosure of cybersecurity insurance held by the organization. I find evidence that the disclosure of cybersecurity insurance is a function of the risk response predisposition of the firm. This is evidenced not only by sentiment, as hypothesized, but also by length of disclosure. Results from this study suggest cybersecurity insurance disclosure as a determinant of subsequent CSB must be interpreted in light of the tone at the top, driving not only the purchase, but also disclosure of voluntary risk transfer. As such, I provide further clarification that the decision to transfer risk is a result of the organizational level risk culture.

I also provide a synthesis of theory and propose a comprehensive framework for understanding IT Risk Culture within the overall IT Governance of an organization (**Figure 9**). I further identify ways in which the elements of Risk Response, one of two IT Risk Culture components, can be measured by disclosed organization activity. Attributable to usage of diverse methodology, I provide a novel identification of three different profiles of IT Risk Culture with respect to risk response – Risk Avoidant, Risk Reduction/Mitigation and Risk Sharing/Transfer.

Figure 9: Theoretical Framework of ITG, IT Risk Management and IT Risk Culture (with measures of analysis)



Organizations identified as predominant Risk Sharing/Transfer IT risk profile are statistically likely to disclose subsequent CSB. These organizations should be a red flag for investors, auditors and members of the supply chain (i.e., economically linked organizations).

Organizations identified as predominant Risk Avoidant IT risk profile should not be assumed low risk for subsequent CSB. Instead, this IT risk profile consists of organizations least likely to make any type of disclosure, including information about subsequent breaches. These organizations have the lowest CSR score and overtly demonstrate a lack of transparency and care for any economically linked organization.

This study is the first to support CSR activity as a key component of an organization's risk management process, specifically a function of ITG. Organizations characteristic of predominant Risk Reduction/Mitigation IT risk profile should correctly be assumed low risk for subsequent CSB. The higher positive sentiment expressed in cybersecurity risk disclosure is in fact a truthful reflection of a proactive IT Risk Culture. I find these are the organizations with the highest CSR activity score, which may explain a strategic choice to invest in sustainable practices and less of a need to invest in cybersecurity insurance to finance costs of any possible subsequent CSB.

Lastly, I contribute greater theoretical understanding of signaling theory within accounting literature, particularly regarding disclosure research. This study demonstrates the differential nature of information signaled via risk disclosure; i.e. characteristics of the organization (IT Risk Culture) as well as likelihood of related subsequent outcome. Due to the timeline of CSB date of incident, identification, investigation and final disclosure, this dissertation provides a unique setting in which to employ signaling theory to evaluate the disparity of information between multiple parties. I find the motivation behind disclosure, as well as considerations for the mandatory nature of disclosure, as critical components to understanding the application of signaling theory within similar studies.

5.2 Practical Contributions

The role of cybersecurity insurance within the IT risk management of an organization has been largely understudied and certainly unclear until this dissertation. I find the propensity to insure is a function of the tone at the top, or ITG, and that the IT Risk Culture – Risk Response is responsible for the signal sent to investors and shareholders regarding the ability of the firm to successfully manage risk. I find evidence to support a holistic view of ITG is appropriate, guiding external users of publicly available data related to cybersecurity to take into consideration multiple characteristics reflective of IT Risk Culture.

Evidence presented in this dissertation suggests the disclosure of cybersecurity insurance by itself is not a statistically significant signal for future breaches or even necessarily significant risk. I provide a framework for disclosed risk response behavior to be used in classification of IT Risk Culture – Risk Response. I find it is IT Risk Culture that provides the best determinants model for future CSB likelihood. Insurance is a preventative internal control by definition, therefore understanding the association between the organization's propensity to mitigate/reduce and avoid risk allows for a more precise interpretation of what insurance disclosure is signaling to investors and shareholders. Understanding the IT Risk Culture of an organization sheds light on the assumption that there is a financial incentive to mitigate a known risk.

Lastly, I demonstrate to audit firms and other risk evaluating services how to utilize information disclosed by an organization to interpret inherent risk. This dissertation provides a guide for how to appropriately utilize cluster analysis; (1) identify cluster variables based on theoretically based similarities, (2) preprocess cluster variables to allow for appropriate cluster interpretation, (3) compare and select the most appropriate clustering algorithm based on the cluster variable data types, and (4) interpret meaningful patterns in cluster variables used to profile different groups of organizations based on cluster membership. Cluster profiles can be utilized to enhance current procedures, as well as accurately assess risk in a holistic approach, in contrast with a single variable prediction model.

5.3 Limitations

I acknowledge certain limitations of my analyses. First, the sample used for this study is limited to U.S. publicly traded organizations from U.S. database sources. As such, the results obtained may not be generalizable to private organizations or those held outside of the country. Second, the data needed for this study is sourced from several different archival databases, which may have missing or incomplete data, and thus result in reduction to sample size. Third, this study is limited to recorded CSB of publicly held organizations. It is likely that there are unrecorded CSB incidents from both public and private firms, each of which I am unable to include in this study. Lastly, it is possible that there are omitted factors which may be associated with IT Risk Culture and CSB which I am unable to measure.

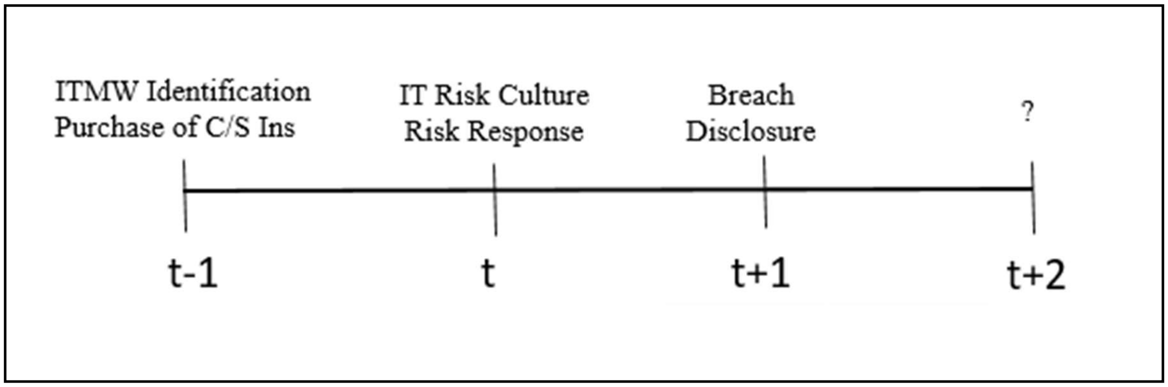
5.4 Future Research

This study contributes to the academic literature on ITG, specifically IT Risk Culture. **Figure 9** provides a depiction of IT Risk Culture components, risk identification and risk response, the latter of which is studied in this dissertation. Future research should explore the risk identification attributes of an organization in order to complete the objective of profiling IT Risk Culture. ICMW was originally hypothesized as a cluster variable in H3, but was found insignificant in predicting IT Risk Culture – risk response. Upon further study, IT_ICMW is likely a better measure for interpreting the risk identification aspect of IT Risk Culture. In accordance with the annual internal control design and implementation process, a comprehensive risk assessment is completed. The ability to identify risk would be evidenced by the effectiveness of IT internal controls. Consequently, future research studying the association between risk identification and risk response is warranted. This research should also improve the ability of IT Risk Culture profiling to assess overall IT risk pertaining to cybersecurity, given the risk response quality is dependent upon the ability to identify risk in need of strategic response.

This dissertation utilizes the disclosure of cybersecurity insurance within the Item 1A Risk Factor cybersecurity risk disclosure as a proxy for the propensity of an organization to share/transfer risk. The decision to share/transfer risk implies a financial incentive to insure vs incur costs from breach. Research studying the association between the purchase of cybersecurity insurance and disclosure would add to the understanding of IT Risk Culture. For instance, it is possible organizations belonging to both Risk Sharing/Transfer and Risk Mitigation/Reduction profiles purchase cybersecurity insurance, but only Risk Sharing/Transfer are likely to disclose. The decision to disclose is possibly related to future litigation risk, whereas a further study would aid in understanding the economic reality of purchasing a cybersecurity insurance policy.

A theorized timeline of breach and IT Risk Culture – Risk Response (**Figure 10**), based on findings from this study, allows for greater insight into how the observations grounded in the IT Governance Framework (**Figure 9**) correspond with organizations experiencing CSB. Further research to determine the timing of breach in association with Risk Identification and Risk Response attributes of IT Risk Culture is needed. Based on the characteristics of the Risk Sharing/Transfer IT risk profile, one of two explanations are possible; either the breach has already occurred at year *t* and not yet been reported or the disclosure behavior is signaling to cybersecurity threat a blueprint of vulnerability and evidence of deep pockets (i.e., cybersecurity insurance). Further research to examine outcomes at year *t*+2 should answer this vital question.

Figure 10: Theorized Timeline of Breach and IT Risk Culture – Risk Response



CSB was included using a binary variable representing either breach in subsequent year following disclosure or no breach. However, organizations can be at risk for different types of breach, internal and external, and perhaps risk response behavior differs based on risk identified with respect to the differing types of breach. An examination of the cybersecurity insurance purchase (implied) and disclosure behavior of breached firms is warranted, with particular focus on which type of breach is most probable to occur in the future. Support for which types of identified cybersecurity risk are more likely to provoke risk transfer/sharing is needed in further understanding IT Risk Culture.

Further analysis regarding the association between CSR activity and type of breach is also warranted. I find a positive, significant interaction effect between CSR activity and cybersecurity insurance disclosure in predicting likelihood of subsequent CSB (**Table 14**). In the complementary cluster analysis results (**Table 19**), I find the average CSR activity score for Risk Sharing/Transfer profile organizations to be high, supporting findings of the regression model. Interestingly, the average CSR activity is higher for Risk Reduction/Mitigation firms which were not found likely to predict subsequent CSB. This collective finding warrants future research to examine the timing of CSR activity and any observations of past breach. For organizations that have experienced past CSB, future research should evaluate any observable change in future CSR activity. These findings also support further research into the potential identification of "greenwashing", which is the use of disclosed CSR activity to act as a cover for known risk or operational failure.

Future research should also examine the type of CSR activity. This dissertation utilized the combined CSR activity score, however, the dimensions of the combined score could also be analyzed; financial, governance, environmental and social. In order to understand the motivation for organizations to invest in CSR activity, it is logical to review the allocation of CSR activity amongst the four dimensions. Analysis of differences between CSR activity dimensions prevalent in Risk Sharing/Transfer organizations compared to Risk Reduction/Mitigation organizations would lend interesting insight into ITG structures that differentially signal subsequent CSB. Triangulation of data between predominant CSR activity dimension, purchase and disclosure of cybersecurity insurance would also further develop theory surrounding IT risk profiles.

Similarly, further understanding of an organization's CSR activity, pre and post breach, in association with its internal control environment is warranted as a result of the findings from this study. CSR activity should inherently improve the efficiency and accuracy of significant processes and policy within an organization. In turn, a review of internal control effectiveness, pre and post breach, would shed light on the claims of this dissertation – that IT Risk Culture is comprised of holistic, interrelated organization attributes, specifically that of risk identification and risk response.

To confirm the findings of Berkman et al. (2018), and to link conclusions from this dissertation, future analysis should evaluate the association between IT Risk Culture prior to CSB and market valuation post CSB. Like Wang et al. (2013), this analysis would provide a comprehensive depiction of how an organization's signals are associated with subsequent outcomes and lend explanatory evidence for market reaction. For example, post CSB, does the market react more or less favorably to firms signaling one IT Risk Culture – risk response compared to another? Additional evaluation of market reaction to different types of IT Risk

Culture absent of review for realized CSB would also lend valuable contribution to related literature.

5.5 Conclusion

I contribute to holistic risk management literature by employing a systems perspective of IT Risk Culture to analyze cybersecurity risk disclosures. Disclosed cybersecurity insurance is for the first time clearly understood as an attribute of IT Risk Culture risk response. When present in a lengthy disclosure with predominantly negative sentiment, disclosure of cybersecurity insurance does in fact signal likelihood of subsequent CSB. Additionally, I provide a novel contribution identifying CSR activity and cybersecurity insurance disclosure together predictive of subsequent CSB. Findings contribute greatly to the understanding of IT Risk Culture classification, predominant risk response behavior and the likelihood of subsequent related outcomes. The value of this knowledge extends to IT risk management, internal and external assurance functions, investors and economically linked organizations.

REFEERENCES

Acquisti, A., et al. (2006). "Is there a cost to privacy breaches? An event study." ICIS 2006 Proceedings: 94.

Aguinis, H. and R. K. Gottfredson (2010). "Best-practice recommendations for estimating interaction effects using moderated multiple regression." Journal of organizational behavior **31**(6): 776-786.

AICPA (2017). "Proposed Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program."

Al Shalabi, L., Shaaban, Z., & Kasasbeh, B. (2006). Data mining: A preprocessing engine. *Journal of Computer Science*, *2*(9), 735-739.

Alawadhi, A., & Byrnes, P. E. (2019). Clustering University Programs in Accounting to Enhance Selection Productivity: Precursor to Recommendation System Development. *Journal of Emerging Technologies in Accounting*, *16*(1), 65-79.

Ali, S., et al. (2015). "Information technology investment governance: What is it and does it matter?" International Journal of Accounting Information Systems **18**: 1-25.

Alpaydin, E. (2020). *Introduction to machine learning*. MIT press.

Amir, E., et al. (2018). "Do firms underreport information on cyber-attacks? Evidence from capital markets." Review of Accounting Studies **23**(3): 1177-1206.

Ballou, B., et al. (2012). "Exploring the strategic integration of sustainability initiatives: Opportunities for accounting research." Accounting Horizons **26**(2): 265-288.

Bandyopadhyay, T., et al. (2009). "Why IT managers don't go for cyber-insurance products." Communications of the ACM **52**(11): 68-73.

Banker, R. D. and C. Feng (2019). "The Impact of Information Security Breach Incidents on CIO Turnover." Journal of Information Systems **33**(3): 309-329.

Bellman, R. (1961). "Adaptive control processes: a guided tour princeton university press." Princeton, New Jersey, USA.

Benaroch, M., et al. (2012). "An internal control perspective on the market value consequences of IT operational risk events." International Journal of Accounting Information Systems **13**(4): 357-381.

Berkman, H., et al. (2018). "Cybersecurity awareness and market valuations." Journal of Accounting and Public Policy **37**(6): 508-526.

Bianchi, D. and O. K. Tosun (2019). "Cyber attacks and stock market activity." Available at SSRN 3190454.

Bodin, L. D., et al. (2018). "Cybersecurity insurance and risk-sharing." Journal of Accounting and Public Policy **37**(6): 527-544.

Bolot, J. and M. Lelarge (2009). Cyber insurance as an incentivefor Internet security. Managing information risk and the economics of security, Springer**:** 269-290.

Boritz, J. E., & Timoshenko, L. M. (2015). Firm-specific characteristics of the participants in the SEC's XBRL voluntary filing program. *Journal of Information Systems*, *29*(1), 9-36.

Bowen, P. L., et al. (2007). "Enhancing IT governance practices: A model and case study of an organization's efforts." International Journal of Accounting Information Systems **8**(3): 191-221.

Byrnes, P. (2019). Automated Clustering for Data Analytics. *Journal of Emerging Technologies in Accounting*.

Campbell, J. L., et al. (2014). "The information content of mandatory risk factor disclosures in corporate filings." Review of Accounting Studies **19**(1): 396-455.

Campbell, K., et al. (2003). "The economic cost of publicly announced information security breaches: empirical evidence from the stock market." Journal of Computer Security **11**(3): 431-448.

Casey, R. and J. H. Grenier (2014). "Understanding and contributing to the enigma of corporate social responsibility (CSR) assurance in the United States." Auditing: A Journal of Practice & Theory, Forthcoming.

Cavusoglu, H., et al. (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.

Cheng, X. and S. Walton (2019). "Do Nonprofessional Investors Care About How and When Data Breaches are Disclosed?" Journal of Information Systems **33**(3): 163-182.

Cheong, A., et al. (2019). "If You Cannot Measure It, You Cannot Manage It: Assessing the Quality of Cybersecurity Risk Disclosure through Textual Imagification." You Cannot Manage It: Assessing the Quality of Cybersecurity Risk Disclosure through Textual Imagification (October 23, 2019).

Cho, C. H., et al. (2015). "CSR disclosure: the more things change…?" Accounting, Auditing & Accountability Journal.

Clarkson, P. M., et al. (2008). "Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis." Accounting, Organizations and Society **33**(4-5): 303-327.

Cohen, J. R., et al. (2004). "The corporate governance mosaic and financial reporting quality." Journal of Accounting Literature: 87-152.

Cohen, J. R. and R. Simnett (2015). "CSR and assurance services: A research agenda." Auditing: A Journal of Practice & Theory **34**(1): 59-74.

Curtis, S. R., et al. (2018). "Consumer security behaviors and trust following a data breach." Managerial Auditing Journal.

Cutler, D. M. and R. Zeckhauser (2004). "Extending the theory to meet the practice of insurance." Brookings-Wharton Papers on Financial Services **2004**(1): 1-53.

Debreceny, R. S. (2013). "Research on IT governance, risk, and value: Challenges and opportunities." Journal of Information Systems **27**(1): 129-135.

Demek, K. C., et al. (2018). "Do organizations use a formalized risk management process to address social media risk?" International Journal of Accounting Information Systems **28**: 31-44.

Ding, K., et al. (2019). "A machine learning-based peer selection method with financial ratios." Accounting Horizons **33**(3): 75-87.

Dye, R. A. (1985). "Disclosure of nonproprietary information." Journal of accounting research: 123-145.

Ehrlich, I. and G. S. Becker (1972). "Market insurance, self-insurance, and self-protection." Journal of Political Economy **80**(4): 623-648.

Ettredge, M., et al. (2018). "Trade secrets and cyber security breaches." Journal of Accounting and Public Policy **37**(6): 564-585.

Ettredge, M. L. and V. J. Richardson (2003). "Information transfer among internet firms: the case of hacker attacks." Journal of Information Systems **17**(2): 71-82.

Feldman, R., et al. (2008). "The incremental information content of tone change in management discussion and analysis."

Feng, C. and T. Wang (2019). "Does CIO risk appetite matter? Evidence from information security breach incidents." International Journal of Accounting Information Systems **32**: 59-75.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 100468.

Gaulin, M. (2017). Risk Fact or Fiction: The Information Content of Risk Factor Disclosures. In: ProQuest Dissertations Publishing.

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

Gharajedaghi, J. (2011). Systems thinking: Managing chaos and complexity: A platform for designing business architecture, Elsevier.

Gordon, L. A. and M. P. Loeb (2002). "The economics of information security investment." ACM Transactions on Information and System Security (TISSEC) **5**(4): 438-457.

Gordon, L. A., et al. (2006). "The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities." Journal of Accounting and Public Policy **25**(5): 503-530.

Gordon, L. A., et al. (2014). "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model." Journal of Information Security **6**(01): 24.

Gordon, L. A., et al. (2015). "The impact of information sharing on cybersecurity underinvestment: A real options perspective." Journal of Accounting and Public Policy **34**(5): 509-519.

Gordon, L. A., et al. (2003). "A framework for using insurance for cyber-risk management." Communications of the ACM **46**(3): 81-85.

Gordon, L. A., et al. (2010). "Market value of voluntary disclosures concerning information security." MIS quarterly: 567-594.

Gordon, L. A., et al. (2011). "The impact of information security breaches: Has there been a downward shift in costs?" Journal of Computer Security **19**(1): 33-56.

Gupta, M. C. and R. J. Huefner (1972). "A cluster analysis study of financial ratios and industry characteristics." Journal of accounting research: 77-95.

Hair, J. F. (2009). Multivariate data analysis.

Haislip, J. Z., et al. (2015). "External reputational penalties for CEOs and CFOs following information technology material weaknesses." International Journal of Accounting Information Systems **17**: 1-15.

Han, S., et al. (2016). "The association between information technology investments and audit risk." Journal of Information Systems **30**(1): 93-116.

Herath, H. S. and T. C. Herath (2008). "Investments in information security: A real options perspective with Bayesian postaudit." Journal of Management Information Systems **25**(3): 337-375.

Higgs, J. L., et al. (2016). "The relationship between board-level technology committees and reported security breaches." Journal of Information Systems **30**(3): 79-98.

Hilary, G., et al. (2016). "Cyber-Risk Disclosure: Who Cares?" Georgetown McDonough School of Business Research Paper(2852519).

Hillman, A. J. and G. D. Keim (2001). "Shareholder value, stakeholder management, and social issues: What's the bottom line?" Strategic Management Journal **22**(2): 125-139.

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

Hosmer, D. W., Jovanovic, B., & Lemeshow, S. (1989). Best subsets logistic regression. *Biometrics*, 1265-1270.

Hummel, K. and C. Schlick (2016). "The relationship between sustainability performance and sustainability disclosure–Reconciling voluntary disclosure theory and legitimacy theory." Journal of Accounting and Public Policy **35**(5): 455-476.

ISACA (2009). "Risk IT. Enterprise risk: Identify, govern and manage IT risk. ." from http://www.isaca.org.

Islam, M. S., et al. (2018). "Factors associated with security/cybersecurity audit by internal audit function." Managerial Auditing Journal.

ITGI (2003). "Board Briefing on IT Governance, Second Edition." (www.itgi.org).

ITGI (2008). "Enterprise value: Governance of IT investments. Getting started with value management. ." (http://www.itgi.org).

Jobst, A. (2007). Operational Risk: The Sting is Still in the Tail But the Poison Dependson the Dose, International Monetary Fund.

Kahyaoglu, S. B. and K. Caliyurt (2018). "Cyber security assurance process from the internal audit perspective." Managerial Auditing Journal.

Kamiya, S., et al. (2018). What is the impact of successful cyberattacks on target firms?, National Bureau of Economic Research.

Karamanou, I. and N. Vafeas (2005). "The association between corporate boards, audit committees, and management earnings forecasts: An empirical analysis." Journal of accounting research **43**(3): 453-486.

Kasznik, R. and B. Lev (1995). "To warn or not to warn: Management disclosures in the face of an earnings surprise." Accounting review: 113-134.

Kearney, C. and S. Liu (2014). "Textual sentiment in finance: A survey of methods and models." International Review of Financial Analysis **33**: 171-185.

Ketchen, D. J. and C. L. Shook (1996). "The application of cluster analysis in strategic management research: an analysis and critique." Strategic Management Journal **17**(6): 441-458.

Kim, D. H. (1999). Introduction to systems thinking, Pegasus Communications Waltham, MA.

Kim, G., et al. (2018). "IT does matter: the folly of ignoring IT material weaknesses." Accounting Horizons **32**(2): 37-55.

Klamm, B. K., et al. (2012). "Determinants of the persistence of internal control weaknesses." Accounting Horizons **26**(2): 307-333.

KPMG (2017). The Road Ahead: The KPMG Survey of Corporate Responsibility Reporting 2017.

Kumar, R. L. (2002). "Managing risks in IT projects: an options perspective." Information & Management **40**(1): 63-74.

Kwon, J., et al. (2013). "The association between top management involvement and compensation and information security breaches." Journal of Information Systems **27**(1): 219-236.

Lawrence, A., et al. (2018). "Is operational control risk informative of financial reporting deficiencies?" Auditing: A Journal of Practice & Theory **37**(1): 139-165.

Li, C., et al. (2012). "THE CONSEQUENCES OF INFORMATION TECHNOLOGY CONTROL WEAKNESSES ON MANAGEMENT INFORMATION SYSTEMS: THE CASE OF SARBANES-OXLEY INTERNAL CONTROL REPORTS." MIS quarterly **36**(1): 179.

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

Li, H., et al. (2017). "Are external auditors concerned about cyber incidents? Evidence from audit fees." Auditing: A Journal of Practice and Theory.

Li, H., et al. (2019) "Data Analytics in Cybersecurity Assurance: Should Data Analytics Be an Integral Part of Cybersecurity Assurance?". (https://zicklin.baruch.cuny.edu/wp-content/uploads/sites/10/2019/12/Data-Analytics-in-Cybersecurity-Assurance-1.pdf)

Li, H., et al. (2018). "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors." International Journal of Accounting Information Systems **30**: 40-55.

Liu, M. C., et al. (2014). "Investigating security investment impact on firm performance." International Journal of Accounting & Information Management.

Loughran, T., & McDonald, B. (2011). When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks. *The Journal of Finance*, *66*(1), 35-65.

Mahoney, L. S., et al. (2013). "A research note on standalone corporate social responsibility reports: Signaling or greenwashing?" Critical Perspectives on Accounting **24**(4-5): 350-359.

McWilliams, A., et al. (2006). "Corporate social responsibility: Strategic implications." Journal of management studies **43**(1): 1-18.

Mukhopadhyay, A., et al. (2019). "Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance." Information Systems Frontiers **21**(5): 997-1018.

Mukhopadhyay, A., et al. (2013). "Cyber-risk decision models: To insure IT or not?" Decision Support Systems **56**: 11-26.

No, W. G. and M. A. Vasarhelyi (2017). "Cybersecurity and continuous assurance." Journal of Emerging Technologies in Accounting **14**(1): 1-12.

O'Donnell, E. (2005). "Enterprise risk management: A systems-thinking framework for the event identification phase." International Journal of Accounting Information Systems **6**(3): 177-195.

Pan, Y., et al. (2017). "Corporate risk culture." Journal of Financial and Quantitative Analysis **52**(6): 2327-2367.

Peterson, R. R. (2004). Integration strategies and tactics for information technology governance. Strategies for information technology governance, Igi Global**:** 37-80.

Rahimian, F., et al. (2016). "Estimation of deficiency risk and prioritization of information security controls: A data-centric approach." International Journal of Accounting Information Systems **20**: 38-64.

Ransbotham, S. and S. Mitra (2009). "Choice and chance: A conceptual model of paths to information security compromise." Information Systems Research **20**(1): 121-139.

Reid, G. C. and J. A. Smith (2000). "The impact of contingencies on management accounting system development." Management accounting research **11**(4): 427-450.

Richardson, V., et al. (2019). "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches." Journal of Information Systems.

Rosati, P., et al. (2019). "Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters." The International Journal of Accounting **54**(03): 1950013.

Sambamurthy, V. and R. W. Zmud (1999). "Arrangements for information technology governance: A theory of multiple contingencies." MIS quarterly: 261-290.

SEC, S. a. E. C. (2011). CF Disclosure Guidance: Topic no. 2: Cybersecurity.

SEC, S. a. E. C. (2018). "Commision Statement and Guidance on Public Company Cybersecurity Disclosures. ."

Shmueli, G. and O. Koppius (2009). "The challenge of prediction in information systems research." Robert H. Smith School Research Paper No. RHS: 06-152.

Skinner, D. J. (1994). "Why firms voluntarily disclose bad news." Journal of accounting research **32**(1): 38-60.

Smith, T. J., et al. (2019). "Do auditors price breach risk in their audit fees?" Journal of Information Systems **33**(2): 177-204.

Spence, M. (1978). Job market signaling. Uncertainty in economics, Elsevier**:** 281-306.

Stanley, L., et al. (2017). "Latent profile analysis: Understanding family firm profiles." Family business review **30**(1): 84-102.

Steinbart, P. J., et al. (2012). "The relationship between internal audit and information security: An exploratory investigation." International Journal of Accounting Information Systems **13**(3): 228-243.

Steinbart, P. J., et al. (2013). "Information security professionals' perceptions about the relationship between the information security and internal audit functions." Journal of Information Systems **27**(2): 65-86.

Steinbart, P. J., et al. (2018). "The influence of a good relationship between the internal audit and information security functions on information security outcomes." Accounting, Organizations and Society **71**: 15-29.

Stiglitz, J. E. (2000). "The contributions of the economics of information to twentieth century economics." The quarterly journal of economics **115**(4): 1441-1478.

Stoel, M. D. and W. A. Muhanna (2011). "IT internal control weaknesses and firm performance: An organizational liability lens." International Journal of Accounting Information Systems **12**(4): 280-304.

Stone, D. N. (2018). "The “new statistics” and nullifying the null: Twelve actions for improving quantitative accounting research quality and integrity." Accounting Horizons **32**(1): 105-120.

Tan, P.-N., Steinbach, M., & Kumar, V. (2016). *Introduction to data mining*. Pearson Education India.

Tanaka, H., et al. (2005). "Vulnerability and information security investment: An empirical analysis of e-local government in Japan." Journal of Accounting and Public Policy **24**(1): 37-59.

Tversky, A. and D. Kahneman (1992). "Advances in prospect theory: Cumulative representation of uncertainty." Journal of Risk and uncertainty **5**(4): 297-323.

Verizon (2020). "2020 Data Breach Investigations Report” (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf)

Verrecchia, R. E. (1990). "Information quality and discretionary disclosure." Journal of Accounting and Economics **12**(4): 365-380.

Wallace, L., et al. (2011). "Information security and Sarbanes-Oxley compliance: An exploratory study." Journal of Information Systems **25**(1): 185-211.

Wang, T., et al. (2013). "The association between the disclosure and the realization of information security risk factors." Information Systems Research **24**(2): 201-218.

Wang, T., et al. (2013). "The textual contents of media reports of information security breaches and profitable short-term investment opportunities." Journal of organizational computing and electronic commerce **23**(3): 200-223.

Weill, P. and J. W. Ross (2004). IT governance: How top performers manage IT decision rights for superior results, Harvard Business Press.

Wilkin, C. L. and R. H. Chenhall (2010). "A review of IT governance: A taxonomy to inform accounting information systems." Journal of Information Systems **24**(2): 107-146.

Wolfe, C. J., et al. (2009). "Concede or deny: Do management persuasion tactics affect auditor evaluation of internal control deviations?" The Accounting Review **84**(6): 2013-2037.

Yen, J.-C., et al. (2018). "The impact of audit firms’ characteristics on audit fees following information security breaches." Journal of Accounting and Public Policy **37**(6): 489-507.

Zyphur, M. J. (2009). "When mindsets collide: Switching analytical mindsets to advance organization science." Academy of management review **34**(4): 677-688.

APPENDIX A: CYBERSECURITY KEY WORDS

Single Words:
failed technology, failed technologies, cyber intrusion, cyberattack, information system, business interruptions, system failure, cyber-attack, information security, cyber incident, cyber attack, data security, breaches of security, computer attack, computer breach, computer break-in, computer security, computer virus, confidential data, confidentiality of data, corruption of data, crimeware, cyber-attack, cyber fraud, cyber incident, cyber insurance, cyber risk, cyber security, cyber terrorist, cyber threat, cyberbased attack, cybersecurity, data breach, data confidentiality, data corruption, data theft, ddos, denial of service, dos, encryption, espionage, hacker, hacking, information attack, information security, information technology, infosec, intrusion, keylogger, keystroke logging, malware, network break-in, network security, phishing, privacy, ransomware, security breach, security incident, social engineering, system security, unauthorized access

Paired Terms[5]:
breach | information system, information technology, information security, data security, cyber security
technology | risks, safeguard
security | compromised, breach, information, information technology, integrity
data | integrity
attack | cyber, IT

[5] Requires the pair of terms within the same subheader.

APPENDIX B: CYBERSECURITY RISK FACTOR EXTRACTION

All available 10-K filings filed between January 2011 to June 2020 were downloaded from the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. In accordance with Campbell et al. (2014) and Gaulin (2017), the design of risk factor disclosure extraction (i.e., Item 1A) is based on the premise that 10-K filings in HyperText Markup Language (HTML) format contain visual clues (e.g., emphasis or whitespace separation). These visual cues are implemented to allow readers the ability to readily recognize item boundaries. The formatting for visual cues are in turn manifested as HTML syntax which is able to be parsed electronically.

Given this ability, the HTML filings are parsed into a tree structure using the AngleSharp package in C# (https://anglesharp.github.io/). Per Li et al. (2018), the tree contains leaf nodes which contain textual information, as well as internal nodes. The internal nodes of the tree contain HTML tags and are used for identifying headings. For example, a tag, <p>, defines a paragraph that is visually separated and isolated from text below and above. By assuming items are presented in order, all the HTML tags that contain the text “ITEM 1A”, “ITEM 1B”, “ITEM 2”, and “ITEM 3” (case insensitive) are identified. From all the candidates, the ones that are emphasized are first selected (i.e., the ones include tag ‘b’, ‘em’, ‘strong’, ‘h1’, ‘h2’, ‘h3’, ‘h4’, ‘h5’, ‘h6’, ‘u’, ‘p’, ‘font’, ‘div’, ‘span’, or ‘li’ if using HTML emphasis tags, or ‘bold’, ‘italic’, ‘underline’, or greater than normal ‘font-weight’ if using Cascading Style Sheets within HTML tags).

Following the procedure, the code generates a list of elements that contain the headers for Item 1A, Item 1B, Item 2, or Item 3. Risk factor disclosures are identified by extracting all the child node contents between the first Item 1A header and the next major section header (Item 1B, Item 2, or Item 3, as in some cases Item 1B or Item 2 are not present). Similar to the approach used in Gaulin (2017) and Li et al. (2018), individual risk factors are also extracted using HTML tags. Per SEC requirements, each unique risk factor must be preceded by a subcaption summarizing the risk. These subcaptions are identified based on such requirement: i.e., they are emphasized (bold, underline, or italic), and are at the beginning of each paragraph or isolated on its own line. Risk factors unique to cybersecurity are identified by containing one or more words from Appendix A within the subcaption. Content between subcaptions represents individual risk factors.