Communications of the Association for Information Systems

Volume 54 Paper in press

2024

# Differential Market Reaction to Data Security Breaches: A Screening Perspective

Shuili Du
*University of New Hampshire*

Kholekile L. Gwebu
*University of New Hampshire*

Jing Wang
*University of New Hampshire*

Kun Yu
*University of Massachusetts Boston*

Communications of the Association for Information Systems

# Accepted Manuscript

## Differential Market Reaction to Data Security Breaches: A Screening Perspective

**Shuili Du**
Peter T. Paul College of Business and Economics
Department of Marketing
University of New Hampshire
0000-0003-3936-4664

**Kholekile L. Gwebu**
Peter T. Paul College of Business and Economics
Department of Decision Sciences
University of New Hampshire
0000-0002-6472-6180

**Jing Wang**
Peter T. Paul College of Business and Economics
Department of Decision Sciences
University of New Hampshire
0009-0008-6677-2405

**Kun Yu**
College of Management
Department of Accounting & Finance
University of Massachusetts Boston
0000-0002-7666-4546

Please cite this article as: Du, S., Kholekile, L. G., Wang, J., & Yu, K. (in press). Differential Market Reaction to Data Security Breaches: A Screening Perspective. *Communications of the Association for Information Systems.*

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

# Differential Market Reaction to Data Security Breaches: A Screening Perspective

**Shuili Du**
Peter T. Paul College of Business and Economics
Department of Marketing
University of New Hampshire
0000-0003-3936-4664

**Kholekile L. Gwebu**
Peter T. Paul College of Business and Economics
Department of Decision Sciences
University of New Hampshire
0000-0002-6472-6180

**Jing Wang**
Peter T. Paul College of Business and Economics
Department of Decision Sciences
University of New Hampshire
0009-0008-6677-2405

**Kun Yu**
College of Management
Department of Accounting & Finance
University of Massachusetts Boston
0000-0002-7666-4546

**Abstract:**

This paper aims to identify breach- and firm-level characteristics that may account for the heterogenous stock market reaction to data breaches. Drawing upon the screening theory, this paper examines the possibility of three breach characteristics (breach severity, breach locus and breach controllability) and two firm attributes (CEO stock ownership, and corporate social responsibility (CSR) performance) serving as information screens to influence stock market reaction to a data breach incident. Using an archival dataset compiled from multiple sources, we examine 607 data breaches from 2004 to 2018 and find that the stock market reacts more negatively if a breach is more severe (i.e., involving more data records and financially sensitive consumer data), controllable (i.e., could have been prevented), and if the breached firm has weak corporate governance, as indicated by low CEO stock ownership. Furthermore, CSR provides an "insurance-like" protection by attenuating the negative effects of breach severity, breach controllability, and poor corporate governance on firm value. Findings of this research highlight the relevance of screening theory as a theoretical lens for examining the contextual dependence of stock market reaction to data breaches on key breach- and firm-level characteristics.

**Keywords:** Data Breach, Screening Theory, Corporate Governance, Corporate Social Responsibility, Abnormal Stock Returns.

[Department statements, if appropriate, will be added by the editors. Teaching cases and panel reports will have a statement, which is also added by the editors.]

[Note: this page has no footnotes.]

This manuscript underwent [editorial/peer] review. It was received xx/xx/20xx and was with the authors for XX months for XX revisions. [firstname lastname] served as Associate Editor.] **or** The Associate Editor chose to remain anonymous.]

# 1 Introduction

Data breach incidents frequently dominate news headlines. With the accelerating development of information technology, cloud computing, and big data, companies are increasingly data intensive and data dependent, and relatedly, face greater concerns about data breach incidents. In 2021, there were over 1000 breach incidents that affected over 298 million individuals (Statista, 2023). Data breaches expose the sensitive personal information of a firm's stakeholders, increasing stakeholders' perceptions of vulnerability to damage from undesired uses of their personal data or identity theft (Martin, Borah, & Palmatier, 2017). Not surprisingly, data breaches trigger negative stock market reaction (Malhotra & Kubowicz Malhotra, 2011; Rasoulian, Grégoire, Legoux, & Sénécal, 2021) and sometimes even the resignation of senior executives who are blamed for the breach incident.

According to a study by IBM (2021), the average total cost of a data breach is 4.24 million USD, with lost business (e.g., cost of lost customers and acquiring new customers, reputational losses, etc.) accounting for the biggest portion of the total cost of a breach. However, despite the overall negative stock market reaction, there exists significant heterogeneity in the stock market reaction to data breaches, with some companies experiencing no decline in stock price whereas others suffer a substantial decline in market value. For example, Malhotra and Malhotra (2011) find that, after a data breach, 34% of firms have positive abnormal returns, and 66% have negative abnormal returns; similarly, Rasoulian et al. (2021) find that the cumulative abnormal returns following a data breach are positive for 40% of firms and negative for 60% of firms. Given the substantial cross-sectional variations in the stock market reaction to data breaches, managers urgently need to gain a deeper understanding of which factors drive the negative impact of data breach on firm value and what firms can do to mitigate such negative effect.

A growing body of literature on data breaches notwithstanding (e.g., Chatterjee, Gao, Sarkar, & Uzmanoglu, 2019; Gwebu, Wang, & Wang, 2018; Janakiraman, Lim, & Rishika, 2018; Malhotra & Kubowicz Malhotra, 2011; Martin et al., 2017), there exists little clarity regarding when, how, and why different breach incidents result in varying magnitudes of negative stock market reaction. Several studies have sought to identify contextual factors that may contribute to the significant heterogeneity in the stock market reaction to data breaches. Nevertheless, these studies have largely been empirically based and lack an adequate conceptual foundation for understanding the financial implication of data breaches. In a piecemeal fashion, they mainly focus on a few contextual factors, and the moderating effects of these factors are equivocal across studies, with some documenting significant effects whereas others showing non-significant effects (Acquisti, Friedman, & Telang, 2006; Gatzlaff & McCullough, 2010; Malhotra & Kubowicz Malhotra, 2011; Martin et al., 2017; Rasoulian et al., 2021).

To address these important limitations, this research employs the screening theory (e.g., Connelly, Certo, Ireland, & Reutzel, 2011; Spence, 1978) as a framework to examine how key breach- and firm-level characteristics may account for the heterogenous stock market reaction to data breaches. The screening theory posits that in the presence of information scarcity and asymmetry, the less informed party will attempt to use various information screens/cues to overcome its information disadvantage and to facilitate improved decision-making (Connelly et al., 2011; Spence, 1978). Following this logic, this research argues that information paucity and asymmetry that shroud a data breach incident make it difficult for investors to ascertain the financial implication of a breach. Further, the stock market often reacts strongly when firms announce a breach, putting pressure on investors to avoid over or underreaction, a common pitfall following an extreme event (Brown & Harlow, 1988). As a result, investors will likely seek out 'screens' to help them differentiate firms whose value will be damaged by the breach from those which will remain unscathed, and subsequently determine how they should respond to a particular breach. Integrating research on crisis management, corporate governance, and corporate social responsibility (CSR) under the common umbrella of the screening theory, this research examines the different paths through which three sources of potential screens may impact the stock market's asymmetric reaction to different breaches, namely breach characteristics (severity, locus, and controllability), CEO stock ownership, and CSR performance. CEO ownership is a key indicator of corporate governance (Sanders & Boivie, 2004) and functions as a screen for investors to infer a firm's unobservable aspects of data security management. As such, the extent of CEO ownership can influence investors' perceptions of data breaches. CSR performance functions as another critical screen because investors can use CSR performance to assess the goodwill and insurance- like protection (Godfrey et al. 2009) the firm has when weathering a data breach crisis. Thus, high CSR performance is likely to reduce the extent of negative stakeholder reaction to the characteristics of the breach. We expect breach characteristics and CEO stock

ownership to directly impact investors' perception of a data breach and, by extension, on stock market reactions, whereas through an alternative path (i.e., the goodwill effect), CSR performance is expected to mitigate the negative impacts of the three breach characteristics and poor corporate governance (i.e., low CEO ownership).

Our work advances data breach research by developing a screening perspective to investigate how key breach- and firm-related characteristics may serve as screens for the stock market to evaluate the financial implication of a breach. The screening theory allows for consideration of an array of contextual factors, thereby providing richer and more realistic insights on when, how, and why the stock market reacts differently to different data breaches. We introduce CEO stock ownership and CSR performance as important screening tools, which have not been studied in the current literature that examines the financial impact of a breach.

The remainder of this article is organized as follows. After reviewing data breach and screening theory literature, we develop our conceptual framework and derive the hypotheses. Subsequently, we explain our event study methodology, the sample, and measurements for the key constructs. We then present the empirical results, followed by a discussion of the theoretical and managerial implications of the research.

# 2 Literature Review

## 2.1 Data Breach, Firm Value, and Stakeholder Reaction

A data breach is an event signaling the potential or actual malpractice of unauthorized access to personal data of a firm's stakeholders (Culnan & Williams, 2009; Rasoulian et al., 2021). Industry reports classify the root causes of data breaches into three categories: (1) system glitches, including both IT and business process failures, (2) human error, including negligent employees or contractors who unintentionally cause a data breach, and (3) attacks by malicious outsiders or insiders (IBM, 2021). Similarly, Rasoulian et al. (2021) identify various causal processes triggering data breaches, ranging from hacker attacks, misplacing data sources, thefts of equipment, to improper disposal and malicious insider attacks.

Prior research has conceptualized data breach incidents as privacy violations (Culnan & Williams, 2009; Martin & Murphy, 2017) or service failures (Malhotra & Kubowicz Malhotra, 2011; Rasoulian et al., 2021) and has documented an overall negative effect of data breaches on firm value (e.g., Acquisti et al., 2006; Gwebu et al., 2018; Martin et al., 2017). However, there are significant cross-sectional variations in stock market reaction to data breach incidents, and our current knowledge on what drives the cross-sectional variations is rudimentary. Several studies have examined contextual variables that affect stock market reaction to data breach incidents, such as firm size, industry, number of affected individuals, and types of breached data (e.g., Acquisti et al., 2006; Malhotra & Kubowicz Malhotra, 2011; Martin et al., 2017; Rasoulian et al., 2021), yet the findings remain inconclusive. For example, Acquisti et al. (2006) find that the negative abnormal stock returns due to data breaches are smaller for large firms and bigger for events affecting more than 100,000 individuals; whereas Malhotra and Kubowicz Malhotra (2011) find that large firms suffer greater market value loss than smaller firms, and that there are no independent effects of the number of affected customers or types of breached data. Martin et al. (2017) find that abnormal stock returns are more negative for breaches with a high number of affected individuals, but that firm size and firm industry type do not have a significant impact on abnormal returns. Further, Rasoulian et al. (2021) find that the abnormal returns to data breach incidents are more negative when breached data contain sensitive information (i.e., financial or SSN or medical information).

In addition to the focus on the stock market reaction to data breaches, another stream of research focuses on stakeholder reactions to data breaches. Chatterjee et al. (2019) find that whether the scope (number of customers affected) of a data breach affects consumer repurchase intention varies depending on the specific emotion, fear or anger, experienced by consumers, as fear and anger elicit different cognitive appraisals of the data breach. Labrecque et al. (2021) find that stress and perceived social contract violations caused by data breaches lead to negative firm-focused behaviors such as negative word of mouth, falsifying information, and switching behavior. Martin et al. (2017) show that data vulnerability affects both the emotional mechanism of violation and the cognitive mechanism of trust, leading to unfavorable consumer behaviors toward the firm.

Although prior research has revealed important insights, the current literature remains empirically based and lacks an adequate conceptual foundation for understanding the drivers of the cross-sectional variations in the stock market reaction to data breaches. Due to the lack of an overarching theoretical

framework, the body of literature in this area tends to be fragmented with a focus on limited contextual factors, hindering the development of a richer and more realistic understanding of when, how, and why different breach incidents result in varying magnitudes of negative stock market reaction. Specifically, prior research has predominantly focused on two breach characteristics (number of individuals impacted and type of data breached) and one firm-level attribute (firm size), although research findings from other fields suggest that other breach characteristics (e.g., locus and controllability of the causes for the breach) (Coombs, 1998; Hartmann & Moeller, 2014; Martin et al., 2017; Rasoulian et al., 2021) and firm attributes (CEO stock ownership and CSR performance) (Bhagat, Brickley, & Lease, 1985; Godfrey, Merrill, & Hansen, 2009a; Sanders & Boivie, 2004; Yermack, 1997) may significantly influence stock market reaction to data breaches. For instance, prior research indicates that the proportion of CEO ownership is associated with abnormal returns and firm value (Bhagat et al., 1985; Sanders & Boivie, 2004; Yermack, 1997) and superior CSR performance can provide "insurance-like" protection for firms during times of crisis (Godfrey et al., 2009a; Klein & Dawar, 2004; Luo & Bhattacharya, 2009; Vanhamme & Grobben, 2009). Omission of important contextual variables will not only limit a fuller understanding of the phenomenon under study, but also lead to the omitted variable bias in the results, which may have partially contributed to the inconsistent findings in prior studies. To address these limitations, a theory driven approach is needed to critically identify a wide range of key breach- and firm related contextual factors and assess the concomitant effects of these factors on the asymmetric negative stock market reactions to data breaches.

## 2.2 Screening Theory

As the counterpart to the signaling theory, screening theory focuses on the implications of information asymmetry on the less informed party of an information market (Connelly et al., 2011; Spence, 1978). In contrast to signaling theory, which is primarily concerned with how parties with an information advantage determine what and how to communicate signals to their advantage in the presence of information asymmetry and scarcity, screening theory focuses on how the less informed party seeks to overcome its information disadvantage by utilizing various forms of screens to facilitate better decision making (Connelly et al., 2011; Spence, 1978). Although the screens used to reduce information asymmetry and uncertainty could come from the signals deliberatively provided by the sender, the less informed party often proactively seeks out screens from alternative sources.

Screening theory has been applied in various contexts to understand how entities, experiencing information asymmetries and paucity, utilize alternative observable screens/cues as substitutes for unobservable characteristics or actions of the focal actor to aid better decision making. For example, banks have been found to use information on employee treatment as a screen to evaluate the unobservable trustworthiness of a borrowing organization when making lending decisions (Qian, Crilly, Wang, & Wang, 2021). Employers use screens such as education to assess the underlying capabilities and qualification of a job candidate in hiring decisions (Weiss, 1995). Managers may also use secondary information cues such as the level of short selling to screen potential B2B partners and make relationship-specific investment decisions (Connelly, Shi, Cheng, & Yin, 2021). Recently, several studies have applied screening theory to gain insights into the stock market reaction of investors. Amidst information asymmetry and scarcity, investors have been found to sift through a myriad of screening cues to identify firms that promise a sound investment. Specifically, investors have been found to use corporate governance characteristics to assess firms' qualitative differences in emerging markets (Sanders & Boivie, 2004). They examine congressional testimonies – witness status, testimony length, and committee jurisdiction – to gauge a firm's political influence (Ridge, Ingram, Abdurakhmonov,& Hasija, 2019), and consider corporate sociopolitical activism statements and actions as proxies for a firm's allocation of resources away from profit-oriented objectives (Bhagwat, Warren, Beck, & Watson, 2020). They monitor changes in block-holding equity stakes to assess the performance prospects of the divesting firm (Bergh, Peruffo, Chiu, Connelly, & Hitt, 2020), consider product market fluidity as an indicator for firm quality, and scrutinize a firm's accruals management as signals for its propensity to obscure its downsizing intentions (Panagopoulos, Mullins, & Avramidis, 2018).

Screening theory is well suited for the purpose of this study due to the lack of information, significant uncertainty, and information asymmetry surrounding a data breach incident. Uncertainty and information scarcity exist because the breach and its investigation could still be ongoing, and even the inflicted firm itself may not know the precise details of the incident (Gwebu et al., 2018). Information asymmetry exists because the inflicted firm possesses private information that is not accessible to the investors although such information is critical in facilitating improved decision making amidst a breach crisis. In the face of

significant information asymmetry, uncertainty, and information paucity, credible signals provided by the breached firm as well as relevant secondary information cues will serve as useful screens to help the market make a sound decision on how it should respond to the different data breaches.

# 3 Conceptual Underpinning

Significant heterogeneity in the stock market's response to data breaches implies that the market sorts the breached firms into different risk strata, selling stocks when perceiving a high financial risk (i.e., the firm's value will be harmed by the breach) but holding or even purchasing more stocks when sensing a low financial risk (i.e., the firm may emerge undamaged by the breach). Because the financial risks of a breach cannot be quantified *ex ante*, the market will likely seek out alternative information screens as proxy indicators that help with the assessment of such risks. According to screening theory, information cues must be observable and perceived as credible and highly correlated with true but unobservable attributes of interest to serve as useful screens (Connelly et al., 2011; Sanders & Boivie, 2004; Weiss, 1995).The logic is that only information cues meeting these criteria can enter a decision maker's calculations. Applying the three criteria, this section discusses why the current study chooses to focus on the three breach characteristics (severity, locus, and controllability) and two firm attributes (CEO stock ownership and CSR performance) as the potential screens that drive the heterogeneous stock market reaction to data breaches.

## 3.1 Breach Characteristics as Screens

In the event of a breach, an announcement is typically issued to disclose the nature of the breach and explain how and why the incident occurred. Naturally, the stock market will first turn to the highly observable signals conveyed in the announcement when assessing the breach's financial risk to the firm. Given the possibility that a breached firm may try to use the breach announcement to influence the public's opinion, the market is expected to rely on signals that are unlikely to be "spun" by the firm. One such signal is the information about the nature of the breach (e.g., the number of records breached, the type of data breached, the cause of the breach, etc.). Such information is objective and is disclosed to the attorney general's office in states where notification of data breaches is mandated by law, holding the breached firm legally liable for manipulating or falsifying this information.

The crisis management literature, including some studies on data breaches, has long suggested that the situational characteristics of a crisis affect stakeholders' cognitive, emotional, and behavioral reactions to the crisis and such characteristics also underlie the influences of the crisis on the focal firm (Hartmann & Moeller, 2014; Martin et al., 2017; Rasoulian et al., 2021). For instance, research drawing on attribution suggests that stakeholders will assign more responsibility to the firm and blame it more if a crisis is (a) triggered by an internal cause, (b) controllable, (c) stable, and (d) more severe (Coombs, 1998; Folkes, 1984; Hartmann & Moeller, 2014), and as a result, stakeholders are more likely to sanction the firm by engaging in unfavorable behaviors such as boycotting, switching brand, reduced spending, and spreading negative word of mouth (Antonetti & Maklan, 2016; Kelley & Michela, 1980; Klein & Dawar, 2004). In the data breach context, the severity of a breach has been found to negatively impact the focal firm's stock price (Acquisti et al., 2006; Martin et al., 2017; Rasoulian et al., 2021). Chatterjee et al.,(2019) find that the severity of a data breach affects repurchase intention when consumers feel fearful. The well-established link between the situational characteristics of a crisis and the various damages inflicted by the crisis on the focal firm suggests that the observable and likely credible breach characteristics can potentially serve as screens to help the market evaluate the unobservable financial risk of the breach. Among other characteristics, severity, locus, and controllability have attracted the most attention in the literature. Thus, the current study focuses on these three characteristics as possible screens that may impact the stock market's reaction to a breach.

*Breach severity* refers to the scope, reach, and impact of a firm's data breach (Chatterjee et al., 2019; Martin et al., 2017) and is related to both the size of the breach (i.e., how many consumers are affected or how many records are compromised) as well as the type of information breached (Malhotra & Kubowicz Malhotra, 2011; Rasoulian et al., 2021).

*Breach locus* captures whether a data breach is caused by an internal or external factor. Internal causes of data breach incidents include malpractice or negligence due to the firm or individual employees, such as insufficient security controls, noncompliance with security policies and procedures, employee negligence, employee theft, or a malicious insider attack (Rasoulian et al. 2021). External causes of data

breach incidents include, for example, a malicious hack from outsiders or the wrongdoing or oversight of a third-party business partner.

*Breach controllability* pertains to whether the firm has reasonable ability or foresight to avoid the breach, in other words, the degree of volitional control the firm has over the breach incident. The "rule of could have done otherwise" (Hamilton, 1980) is relevant here. The underlying assumption of controllability is that a firm is an autonomous chooser between courses of action; to the degree that the breach results from a course of action the firm has volitionally chosen over other alternatives, the breach is controllable and, to an extent, preventable. When a firm is perceived to have reasonable foresight and/or ability to avoid the data breach, or when a firm could have done otherwise to prevent the breach but did not do the right thing (e.g., establish a strict IT security policy and enforce strict data security compliance among employees and third-party business partners), breach controllability is perceived as high.

It is important to note that locus and controllability are two conceptually distinct constructs (Kelley & Michela, 1980; Weiner, 1980) and are empirically distinguishable (Folkes, 1984; Folkes, Koletsky, & Graham, 1987; Hartmann & Moeller, 2014; Klein & Dawar, 2004). The former is concerned solely with the breach's origin, with no consideration for the firm's capability to prevent or control it. The latter addresses the firm's capability and opportunity to prevent a data breach, irrespective of whether the breach originates internally or externally. Thus, the correlation between locus and controllability isn't direct or automatic. To illustrate, within both the internal and external locus categories, there's a wide range of causes for data breaches, each with different levels of controllability. An internal breach due to employees' malicious acts may be less controllable than an internal breach due to lack of proper security policies. The latter, being a systemic issue, can be avoided/controlled by improving and enforcing robust security measures, while the former, often shrouded in intentional deceit and disguise, remains challenging to predict or prevent. External breaches similarly range in controllability. A sophisticated cyber-attack, especially one executed by well-resourced adversaries deploying advanced techniques, often eludes even robust security defenses, rendering it less controllable. Conversely, a breach resulting from a third-party's noncompliance with security protocols can be more easily mitigated by enforcing stricter standards and compliance mandates. The low correlation found between locus and controllability in our subsequent correlation analysis provides empirical support for the assertion that these two constructs are conceptually distinct (see Table 3).

## 3.2 Corporate Governance (CEO Stock Ownership) as a Screen

Data breaches are typically not random occurrences. Instead, they stem from underlying causes ranging from the firm's myopic, and opportunistic strategies with information security management to its mismanagement of information security resources and capabilities. Breach characteristic information reveals more symptoms than the root causes of the breach, falling short of shedding sufficient light for the market to comprehensively assess the financial risks of a breach. By contrast, firm-level attributes will likely convey more fundamental information on firm strategies and management conduct.

Firms are unlikely to reveal to outsiders sensitive information involving their security management related strategies, initiatives, and capabilities (Kotulic & Clark, 2004) although such information is vital for the market to identify the root cause of a breach and to comprehensively assess the financial risks of the breach. Lacking such information, the market is likely to search for alternative, credible, and observable screens such as corporate governance to compensate for the lack of desired information. We focus on CEO stock ownership, as it is the key indicator of corporate governance. Agency theory (Currim, Lim, & Kim, 2012; Jensen and Meckling, 1976) suggests that CEO ownership reflects the alignment between the interests of shareholders and those of the CEO, which is the fundamental issue of modern corporations. Through gain and loss sharing, a high proportion of CEO stock ownership aligns CEOs' wealth with shareholder value, thereby incentivizing CEOs to implement corporate strategies and policies that maximize shareholder value and thwarting myopic, opportunistic behaviors (Currim, Lim, & Kim, 2012; Jensen & Meckling, 1976; Sanders & Boivie, 2004). By contrast, a low proportion of CEO ownership increases agency cost and encourages myopic behavior and executive opportunism. Accordingly, firms with high (vs. low) CEO ownership are believed to have better (vs. poor) corporate governance.

Consistent with this line of research, high CEO stock ownership, due to better corporate governance (Mehran, 1995), may serve as a screen to substitute the unobservable indicator of the high quality of a firm's data security management, in the sense that firms with high CEO stock ownership are believed to implement effective strategies and eschew opportunistic mismanagement to strengthen the firm's data security management capabilities. Conversely, low CEO stock ownership, due to poor corporate

governance, would serve as a proxy for the unobservable indicator of the low quality of a firm's data security management, because firms with low CEO stock ownership tend to be more prone to myopic behavior and executive opportunism when managing their data security resources and capabilities. In summary, corporate governance, as captured by CEO stock ownership, conveys observable and credible information about firm quality related to data security management that may help the market appraise the financial risks of a breach, and thus may serve as a screen to impact the stock market's reaction to data breaches.

### 3.3 CSR Performance as a Screen

CSR is defined as the extent of a firm's commitment to improving economic, social, and environmental wellbeing through business practices, policies, and resources (Kotler & Lee, 2005). Through socially responsible activities, a firm demonstrates its cultural allegiance to the society's institutional norms and attains legitimacy and stakeholder support (Scott, 1987; Suchman, 1995). Research shows that firms with higher CSR performance benefit from stronger stakeholder support (Sen, Du, & Bhattacharya, 2016; Torres, Bijmolt, Tribó, & Verhoef, 2012); for example, socially responsible firms enjoy higher customer trust and loyalty (Du, Bhattacharya, & Sen, 2011; Park, Kim, & Kwon, 2017; Sen et al., 2016; Walsh & Bartikowski, 2013), attract better talent, and are better able to motivate and retain their employees (Surroca, Tribó, & Waddock, 2010; Turban & Greening, 1997).

Godfrey et al. (2009a) propose that CSR programs may generate positive moral capital among communities and stakeholders, and such moral capital can provide "insurance-like" protection for the firm, especially during times of crisis. Specifically, Godfrey (2005) argues that superior CSR performance enables the firm to gain insurance-like protection in two ways: (1) the degradation of relationship-based intangible assets is tempered by positive moral capital (e.g., loyalty suffers to a lesser extent), and (2) stakeholders impose less severe sanctions on the firm than in the absence of positive moral capital. Several studies have provided empirical evidence for CSR's ability to provide insurance-like protection at either the firm level or stakeholder level (e.g., Godfrey et al., 2009a; Klein & Dawar, 2004; Luo & Bhattacharya, 2009; Vanhamme & Grobben, 2009).

CSR performance information is widely accessible through various publicly available CSR ratings. Being rated by external parties, CSR performance data will likely be perceived favorably in terms of its credibility. CSR performance also has a perceived link, validated by the empirical evidence from the CSR literature, with true, but unobserved underlying quality and integrity of a firm that provides the firm with insurance-like protection during times of crisis. In the event of a breach, CSR performance qualifies as a useful screen to help the market distinguish firms with lower financial risks, those protected by their favorable CSR record, from firms with higher financial risks, those not protected due to poor CSR performance.

## 4 Conceptual Model and Hypothesis Development

Figure 1 presents the conceptual model of market reaction to a data breach. The model posits that breach characteristics (i.e., severity, locus, and controllability) and CEO stock ownership directly impact market reaction to a data breach. With its "insurance-like" effect, CSR performance is expected to moderate the effects of breach characteristics and CEO stock ownership on the stock market's reaction to data breaches. Although both CEO stock ownership and CSR performance are firm-level attributes, we expect them to function differently to influence market reactions to data breaches. CEO stock ownership, being a key indicator of corporate governance, operates as a screen through which the unobservable quality and financial risk associated with a firm's data security management can be assessed. Thus, CEO stock ownership directly shapes the market's perception of the breach. All else being equal, lower CEO stock ownership, indicative of weaker corporate governance, leads to a more negative market perception of the breach due to presumed weaker data security management and misaligned CEO interests. In contrast, CSR, with its broader focus on societal and environmental wellbeing (Kotler & Lee, 2005), serves as a screen for assessing the risks faced by a breached firm based on the firm's goodwill and its insurance-like protection during times of a breach crisis (Godfrey et al. 2009a). In cases where the breach's negativity remains consistent (e.g., in terms of severity and controllability), stakeholders tend to impose less sanctions on firms with higher CSR performance. Supporting this argument, prior research (Luo and Bhattacharya 2009) suggests that CSR as a screen does not directly influence the negativity of the market's perception of a breach but rather mitigates the effect of negative perception of a breach. We elaborate more on these arguments in subsequent sections.

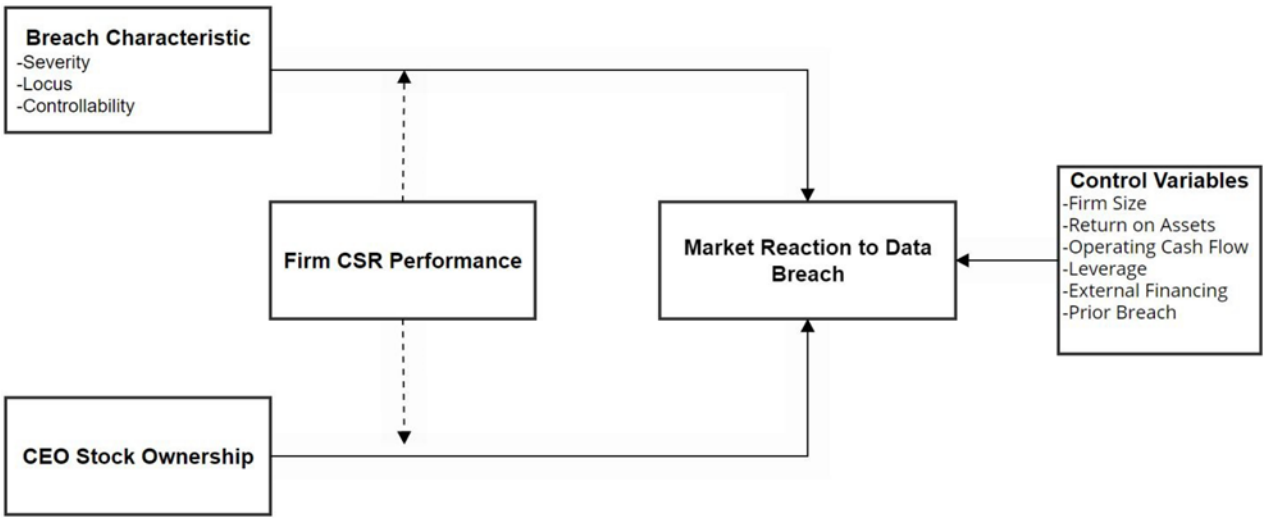


**Figure 1. A Conceptual Model of Market Reaction to Data Breaches**

## 4.1 Breach Characteristics

The crisis management literature has consistently demonstrated that crisis characteristics underlie the impacts of the crisis on the focal firm and influence stakeholders' cognitive and emotional appraisals of the crisis. Moral judgment, blame, and stakeholder sanctions against the focal organization are likely to intensify when a crisis is perceived as severe, caused by an internal factor, and controllable (Lange & Washburn, 2012). Prior research suggests that when a negative incident is controllable or caused by internal factors, or the harmful outcomes are severe, individuals are more likely to view questionable practices as unethical and unfair (Barclay, Skarlicki, & Pugh, 2005; Gino, Shu, & Bazerman, 2010; Mudrack & Mason, 2013; Vitell, 2003) and attribute more blame to the firm (Laufer, Gillespie, McBride, & Gonzalez, 2005). So much so that individuals are more likely to demonstrate negative emotional reactions (Xie, Bagozzi, & Grønhaug, 2015) and retaliate against the firm, resulting in negative word-of-mouth, complaining, reduced spending, and switching and boycotting (Antonetti & Maklan, 2016; Kelley & Michela, 1980; Klein & Dawar, 2004).

A breach incident is frequently cloaked in uncertainty, incomplete information, and information asymmetry. In such information starved contexts, the well-established empirical evidence linking crisis severity, controllability, and internal locus to the damages inflicted on the focal firm allows the market to use the three breach characteristics as screens to filter the breached firms into different risk strata, reacting more negatively to breaches that are riskier (severe, controllable, and internally caused). Therefore, we propose the following hypotheses.

**Hypothesis 1: All else equal, the decline in market value due to a data breach is larger for breaches that are more severe.**

**Hypothesis 2: All else equal, the decline in market value due to a data breach is larger for breaches that have an internal locus of causality.**

**Hypothesis 3: All else equal, the decline in market value due to a data breach is larger for breaches that are more controllable.**

## 4.2 CEO Stock Ownership

The heterogeneity in the stock market's reaction to data breaches reflects the stock market's belief that breaches pose varying levels of financial risks for the firm. As previously discussed, CEO stock ownership, a highly observable cue, communicates valuable information on firms' strategic choices, initiatives, and practices regarding information security management. In this sense, CEO stock ownership may serve as a screening proxy for the quality of the breached firm's corporate governance (hidden strategies, practices, and capabilities) with regard to data security, to the extent that a higher (vs. lower) level of CEO stock ownership denotes better (vs. poorer) corporate governance, and consequently higher (vs. lower) data security management capabilities. More specifically, CEO stock ownership has the potential to act as a

diagnostic screen for the stock market to sort the breached firms into different risk strata through the following two channels.

First, CEO ownership may serve as an indirect but observable information cue that is indicative of a firm's underlying quality. Investors are likely to perceive firms with higher levels of CEO ownership as being of higher quality (Sanders & Boivie, 2004), because greater stock ownership by CEOs reduces agency conflicts and allows risk sharing between shareholders and the CEO (Jensen and Meckling, 1976). Empirical evidence shows that data breaches cause significant financial damage to shareholder value (Acquisti et al., 2006; Gwebu et al., 2018; Martin et al., 2017). Since CEO stock ownership is directly correlated with the magnitude of financial losses suffered by the CEO when firm value decreases, CEOs with larger stockholdings have more to lose should a breach afflict the firm. Therefore, a CEO with a higher stake in the firm may be more motivated to implement effective strategies and shun opportunistic mismanagement to build robust data security management capabilities (Jensen & Meckling, 1976; Zhang & Wiersema, 2009). In the event of a breach, the strength of the firm's data security management capability will in turn increase the likelihood that the firm will swiftly overcome the breach, consequently lowering the financial risks associated with the breach. Therefore, the market is expected to respond more (less) negatively to data breaches at firms with lower (higher) levels of CEO stock ownership.

Second, CEO ownership may also serve as managerial certification of firm quality and reflect CEO competency (Sanders & Boivie, 2004) and CEO credibility (Zhang and Wiersema 2009). Investors may infer from the CEO's acceptance of large stock ownership that the CEO is confident about the firm's financial prospects and that the CEO is talented and competent in reducing firm risk and maximizing future cash flows. As a result, the market may perceive a higher (vs. lower) financial risk related to data breaches and thus respond more (vs. less) negatively to firms with lower (vs. higher) levels of CEO ownership. Taken together, CEO ownership may serve as a potential screen for the market to infer firm quality and CEO competency, and thus helps the market sort breach firms into different risk strata. Our fourth hypothesis is summarized below as follows:

**Hypothesis 4: All else equal, the decline in market value due to a data breach is larger for firms with lower CEO stock ownership.**

## 4.3 The Buffering Effect of CSR in Stock Market Reaction to Data Breach

As previously discussed, in the event of a breach, CSR performance functions as a useful screen to help the market sort firms into varying risk strata based on the extent of "insurance-like" protection afforded by their CSR record. A favorable CSR record reduces the perceived financial risk of a breach, whereas a poor record increases the perceived financial risk. Therefore, we expect that, for a firm with a superior CSR record, due to the perception of reduced financial risks, the market is more inclined to discount or downplay the unfavorable breach characteristics (i.e., the breach is severe, internal, or controllable) and low CEO ownership, and be less influenced by such information in its subsequent decision to sanction the firm. In contrast, for a firm with an inferior CSR record and thus a little reservoir of goodwill, the market will perceive the breach as riskier and consequently impose more severe sanctions when the breach characteristics and the firm's CEO ownership are unfavorable. These arguments suggest that a positive record of CSR performance will reduce the negative effects of severity, locus, controllability, and CEO ownership on firm value.

Supporting this reasoning, research at the intersection of CSR and relationship marketing suggests that a firm's CSR activities signal its "warmth", which refers to traits such as being caring, helpful, and being concerned about the needs and welfare of its stakeholders and the society at large (Bolton & Mattila, 2015; Kervyn, Fiske, & Malone, 2012). Such warmth perceptions speak to the firm's enduring values and underlying character and are particularly important in the context of a negative event (e.g., a data breach), causing the stock market to perceive the breach as less risky and to discount the informational value of the breach characteristics and CEO ownership when they are negative (i.e., the breach is severe, internal, and controllable and CEO ownership is low) (Dawar & Pillutla, 2000). Relatedly, Bhattacharya and Sen (2003) argue that CSR helps a firm cultivate strong stakeholder identification with the firm, that is, stakeholders' perception of "oneness or belongingness" with the firm. Such CSR-based identification underlies strong, committed, and meaningful relationships between the firm and its stakeholders (Du, Bhattacharya, & Sen, 2007) and is likely to dispose the market to overlook or downplay the importance of the three breach characteristics and mitigate the negative effect of low CEO stock ownership (Bergami & Bagozzi, 2000; Bhattacharya & Sen, 2003), thereby reducing their negative effects on firm value.

**Hypothesis 5: All else equal, the negative effects of (a) breach severity, (b) breach internal locus, (c) breach controllability, and (d) low CEO ownership on the firm's market value are smaller for firms with high CSR performance than for firms with low CSR performance.**

# 5 Conceptual Methodology

## 5.1 Sample

Our sample consists of data breach announcements made by publicly traded firms for the period 2004-2018. The data breach announcements are drawn from the Open Source Foundations DatalossDB database and the Privacy Clearinghouse data breach database, which gathers data breach announcements from multiple sources, including various media outlets, state Attorney General's Office's breach records, and the U.S. Department of Health and Human Services. The initial sample includes 8,979 breach announcements from a vast array of organizational types including medical institutions, businesses, educational institutions, government, and military and nonprofits. We merge firm's breach announcement data with CSR performance information from MSCI KLD, financial information from Compustat, stock return information from Center for Research in Security Prices (CRSP), and CEO ownership from Compustat Execucomp. We exclude observations with missing data for required variables. Finally, to avoid the influence of confounding events, we eliminated the announcements if there were mergers or acquisitions surrounding the announcement of the breach incident. The final sample consists of 607 observations for 304 unique firms from 2004 to 2018.

Table 1 Panel A reports the distribution of breach announcements by year, with years 2006-2008 having the most breach announcements. Panel B reports the distribution of breach announcements by industry. The Finance, Insurance, and Real Estate industry has the greatest number of breach announcements, accounting for 34.6% of the sample. The Service (hotel, personal, business, etc.) industry and the Wholesale and Retail Trade industry account for 18.78% and 17.30% of the sample, respectively.

**Table 1. Sample Distribution**

*Panel A- Breach Announcements by Year*

| Year | Freq. | Percent |
|---|---|---|
| 2004 | 3 | 0.49 |
| 2005 | 15 | 2.47 |
| 2006 | 73 | 12.03 |
| 2007 | 72 | 11.86 |
| 2008 | 75 | 12.36 |
| 2009 | 45 | 7.41 |
| 2010 | 68 | 11.20 |
| 2011 | 31 | 5.11 |
| 2012 | 33 | 5.44 |
| 2013 | 26 | 4.28 |
| 2014 | 50 | 8.24 |
| 2015 | 27 | 4.45 |
| 2016 | 34 | 5.60 |
| 2017 | 30 | 4.94 |
| 2018 | 25 | 4.12 |
| **Total** | **607** | **100.00** |

*Panel B- Breach Announcements by Industry*

| Industry | SIC code | No. of obs. | Percent |
|---|---|---|---|
| Mining and construction | 1000-1999 | 8 | 1.32 |
| Non-Durable Manufacturing | 2000-2999 | 34 | 5.60 |
| Durable manufacturing | 3000-3999 | 60 | 9.88 |
| Transportation, Communications, and Utilities | 4000-4999 | 56 | 9.23 |
| Wholesale and Retail Trade | 5000-5999 | 105 | 17.30 |
| Finance, Insurance and Real Estate | 6000-6999 | 210 | 34.60 |
| Service (hotel, personal, business & etc.) | 7000-7999 | 114 | 18.78 |
| Service (health, legal, educational & etc.) | 8000-8999 | 16 | 2.64 |
| Public administration | >8999 | 4 | 0.66 |
| Total | | 607 | 100.00 |

## 5.2 Measuring Stock Market Reaction to Data Breach

We evaluate the stock market reaction to data breach announcements using an event study methodology and perform multiple regressions to test our hypotheses. In an efficient market, abnormal changes in stock price over a short time period surrounding a data breach announcement should reflect investors' assessment of the financial impact of the breach based on all publicly available and relevant information (Gwebu et al., 2018). We use the date of breach disclosure as the event date and compute market-adjusted daily abnormal returns. Specifically, the model below is estimated for each firm during the 150-day estimation period, beginning 159 trading days before the breach announcement date and ending 10 trading days prior to this date.

$$R_{id} = \alpha_i + \beta_i R_{md} + \varepsilon_{id} \quad (1)$$

Where $R_{id}$ denotes the stock return for firm *i* on day *d*, $R_{md}$ is the return on the CRSP value-weighted market portfolio on day *d*, and $\varepsilon_{id}$ is the residual of the estimation. The abnormal return for firm *i* on day *d* ($AR_{id}$) is estimated as:

$$AR_{id} = R_{id} - (\hat{\alpha}_i + \hat{\beta}_i R_{md}) \quad (2)$$

where $\hat{\alpha}_i$ and $\hat{\beta}_i$ are the parameter estimates of $\alpha_i$ and $\beta_i$ obtained from equation (1). Cumulative Abnormal Returns (CAR) are computed by summing individual abnormal returns over a seven-day window (-3 to +3) around the breach announcement date. Thus, CAR is computed as:

$$CAR_{i(-3,3)} = \sum_{d=-3}^{3} (AR_{id}) \quad (3)$$

## 5.3 Measuring Breach Characteristics

This study focuses on three primary characteristics of data breaches: breach severity, locus, and controllability.

***Breach Severity*:** Breach severity captures the scope, reach, and impact of a firm's data security breach (Martin, Borah, & Palmatier, 2017). A data breach is more severe if it involves a large number of compromised records or if it involves stakeholders' sensitive information. Accordingly, we measure two aspects of breach severity, the quantitative aspect (i.e., the number of records breached) and the qualitative aspect (i.e., whether the breach data is sensitive). Conceptualization of sensitive data often includes financial data (i.e., debit card, bank account information), social security number (SSN), medical information, and identification information (i.e., name, driver's license number, date of birth; Malhotra and Malhotra 2011; Rasoulian et al. 2021). Rasoulian et al. (2021) find that financial data breaches result in significantly negative stock market reactions, whereas the effect of breaches involving SSN or medical information on stock price is weak or inconsistent. In line with prior research, *Severity Quantitative* is measured by the log transformed value of 1 plus the number of records breached. We focus on financial information for the qualitative aspect of breach severity and assess whether the breached information includes financial data in our main analysis. More specifically, *Severity Qualitative* is coded as 1 if the

breach announcement contains key words such as bank, debit card, routing, check, loan, mortgage, financial fraud/criminal, tax, investor, and broker, and 0 otherwise. We include the variations of each keyword in our search. For example, we search for bank, banks, and banking to identify breaches related to bank information. In our additional analysis, we use an alternative measure of *Severity Qualitative* by assessing whether the data breaches involve personal/medical information.

***Breach Locus Internal*****:** Locus of causality pertains to whether the data breach is caused by an internal factor (e.g., an employee or the firm) or an external factor (e.g., a malicious hacker, negligence by a contractor) (Rasoulian et al. 2021). Based on the data breach announcements, we code breach *Locus Internal* as 1 if a breach originated from a source within the firm, such as employees or associates, and 0 otherwise.

***Breach Controllability*****:** Breach controllability relates to the degree of volitional control the firm has over the breach incident. We developed our coding for controllability based on prior research (e.g., Burnett 1999; Hansman and Hunt 2005; Rasoulian et al. 2021). A breach is classified as "controllable" and coded as 1 when it results from factors such as errors, mistakes, accidents, policy violations, inadequate security controls, or vulnerabilities that could have been avoided by the breached firm or relevant third parties. Such factors may encompass incidents like incorrect disposal, loss, misplacement of documents/IT assets, security policy violations, and vulnerabilities arising from insufficient implementation and enforcement of robust security controls, policies, and procedures (Rasoulian et al. 2021). Conversely, a breach is categorized as "noncontrollable" and coded as 0 when it originates from circumstances that largely evade preventive measures. Such noncontrollable breaches may encompass situations like highly sophisticated cyberattacks executed by well-resourced threat actors or even instances of malicious insider threats posed by employees, where the firm's capacity for anticipatory control is limited.

***Inter-Rater Reliability Assessment:*** Two independent raters reviewed the breach announcements and coded the breaches based on the presence of sensitive information, whether they originated internally or externally, and their controllability. To assess the inter-rater reliability of this coding process, a Cohen's Kappa statistical test (Cohen, 1960) was conducted. A Kappa (κ) statistic of zero indicates only slight agreement between raters, while a value exceeding 0.8 indicates an exceptional level of agreement (Landis & Koch, 1977). The results of the statistical analysis demonstrated high levels of inter-rater reliability, as evidenced by the following Kappa (κ) statistics: sensitivity (κ = 0.94), locus (κ = 0.88), and controllability (κ = 0.95). Finally, in line with the approach outlined by Gerstner and Day (1997), any discrepancies in coding were resolved through discussion between the raters, ultimately resulting in complete agreement.

## 5.4 Measuring CEO Ownership and CSR Performance

CEO stock ownership is defined as the percentage of total shares owned by the CEO obtained from Compustat Execucomp. We derive our measure of firm CSR performance from the MSCI KLD database, which tracks the social and environmental performance of the 3,000 largest U.S. publicly traded firms and has been widely used in scholarly research to measure CSR performance (Dhaliwal et al. 2011; Du et al., 2017; Servaes & Tamayo, 2013; Waddock and Graves, 1997). The KLD database provides annual data on firms' positive (i.e., strengths) and negative (i.e., concerns) performance in the areas of environment, community, diversity, employee relations, human rights, and product quality and safety. For each domain, there are multiple indicators for strengths and concerns. For example, for the community domain, there are eight strengths and six concerns indicators. To arrive at ratings for each social and environmental domain, independent analysts and rating experts at KLD utilize information from a variety of sources, including both corporate and independent external sources. Corporate data sources include standalone corporate sustainability reports, completed yearly questionnaire about sustainability practices, corporate quarterly and annual reports; external data sources include general business press (e.g., Business Week, Wall Street Journal), trade magazines, regional Environmental Protection Agency newsletters, specialized periodicals such as Chronicles of Philanthropy, government surveys, and so on (Du et al. 2017).

Following prior research (Du et al., 2017; Godfrey, Merrill, & Hansen, 2009b; Servaes & Tamayo, 2013), we obtain CSR scores for each firm-year by subtracting the number of concerns from the number of strengths across the domains of community, diversity, employee relations, environment, and product quality. We then use the scaled decile ranks of CSR scores as our measure of CSR performance (*CSR*) in the regression analysis to facilitate the interpretation of the regression results and to allow for the

nonlinear effects of CSR performance (Du et al. 2017; Bartov et al. 2021). In particular, *CSR* is calculated by ranking the CSR scores for each year into ten groups (0 to 9) by decile points and then dividing the group numbers by nine, so that the scaled rank ranges between zero and one.

### 5.5 Control Variables

Multiple control variables are incorporated into the model to account for possible confounding influences. These include firm size (*SIZE*), the return on assets (*ROA*), operating cash flows (OCF), financial leverage (*LEV*), financing needs (*FIN*), whether the firm has prior breaches (*PRIOR*), and time and industry fixed effects.

***SIZE***: SIZE is defined as the natural logarithm of total assets. Some prior studies have found that the magnitude of abnormal returns following a breach announcement varies significantly depending on firm size, although the exact effect of firm size on abnormal returns to data breaches is mixed (Gatzlaff and McCullough 2010; Malhorta and Malhortra 2011; Martin et al. 2017).

***ROA and OCF*****:** *ROA* is the return on assets, computed by dividing income before extraordinary items by total assets. *OCF* is operating cash flows scaled by total assets. We include *ROA* and *OCF* to control for the impacts of firms' financial performance on investors' reactions to data breaches. Firms with better financial performance are likely to have more resources available for investments in processes and tools that can potentially prevent future data breaches (Kashmiri, Nicol, & Hsu, 2017). As a result, investors may perceive data breaches by firms with higher *ROA* and *OCF* as less severe and react to such breaches less negatively.

***LEV and FIN*****:** *LEV* is financial leverage, defined as total liabilities divided by total assets. *FIN* captures firms' needs for external financing, calculated as the sum of equity financing (i.e., the sale of common and preferred shares minus the purchase of common and preferred shares) and debt financing (i.e., the long-term debt issuance minus the long-term debt reduction) scaled by total assets (Dhaliwal et al. 2011). Boasiako and Keefe (2021) suggest that data breaches may increase credit risk and make it difficult for firms to obtain external financing from the market. Firms with higher financial leverage and needs for external financing are more likely to be financially constrained and adversely affected by data breaches, suggesting more negative abnormal returns around breach announcements.

***PRIOR:*** *PRIOR* is an indicator variable, equal to 1 if the firm has had prior data breaches and 0 otherwise. Prior breaches may affect investors' perception of and reaction to the current breach (e.g., Gwebu et al. 2018).

***Time and Industry Fixed Effects*****:** To account for time effects, we include year dummies in the model. Similarly, industry dummies are included to account for industry-level variance.

## 6 Empirical Results

### 6.1 Descriptive Statistics

Panel A of Table 2 shows the descriptive statistics for cumulative abnormal returns (*CAR*) for different time windows. Both the mean (-0.38%, $p < 0.01$) and the median (-0.26%, $p < 0.01$) of *CAR* during the 3-day event window (-1, 1) are significantly negative, suggesting that the stock market reacts negatively to data breaches on average. This is consistent with prior studies showing that the announcements of data breach incidents result in reduced firm value (Malhotra and Malhotra 2011; Martin et al. 2017; Rasoulian et al. 2021). Furthermore, the mean and the median of *CAR* become more negative for the event windows (-2, 2) and (-3, 3), consistent with the argument that there may be some information leak before breach announcements and that it may take time for the market to digest the impacts of data breaches (Goel and Shawky 2009; Malhotra and Malhotra 2011). We thus focus on *CAR* during the 7-day event window (-3, 3) in our regression analysis. In addition, we also compute the *CAR* before and after the (-3, 3) event window. Both the mean and the median of *CAR* during the time windows (-9, -4) and (4, 9) are not significant, suggesting that the negative market reaction during the (-3, 3) event window is not produced by unrelated trends surrounding the event dates.

Next, we examine the cumulative abnormal returns around breach announcements conditional on CSR performance. In particular, we construct two subsamples based on the median of CSR performance. The high (low) CSR performance subsample contains firms with CSR performance above (at or below) its median. The *CAR* for the event windows (-1 ,1), (-2, 2) and (-3, 3) for each subsample are reported in Panel B of Table 2. While there is no significant difference in *CAR* (-1, 1) between the two subsamples, firms with high CSR performance exhibit significantly less negative cumulative abnormal returns for event windows (-2, 2) and (-3, 3) than those with low CSR performance.

The descriptive statistics for the independent variables in our multivariate analysis are shown in Panel C of Table 2. About 22.6% of data breaches in our sample are related to sensitive financial data, 14.7% of data breaches are caused by an internal factor (i.e., internal locus), and 23.4% of data breaches are controllable. The average CEO stock ownership is .52%.

**Table 2. Descriptive Statistics**

Panel A: Cumulative abnormal returns for different time windows

| Day(s) | CAR | | | | | | |
|---|---|---|---|---|---|---|---|
| | Mean | (p value) | Median | (p value) | Q1 | Q3 | Std. Dev. |
| (-9, -4) | 0.11% | (0.483) | 0.03% | (0.626) | -1.71% | 2.19% | 0.040 |
| (-1, 1) | -0.38% | (0.004) | -0.26% | (0.005) | -1.69% | 1.08% | 0.032 |
| (-2, 2) | -0.63% | (0.001) | -0.33% | (0.019) | -2.11% | 1.29% | 0.046 |
| (-3, 3) | -0.75% | (0.000) | -0.36% | (0.012) | -2.40% | 1.56% | 0.051 |
| (4, 9) | 0.10% | (0.592) | 0.12% | (0.330) | -1.91% | 2.08% | 0.045 |

Panel B: Cumulative abnormal returns conditional on CSR performance

| | Low CSR Performance | High CSR performance | Difference (2) – (1) | p-value |
|---|---|---|---|---|
| CAR (-1, 1) | -0.44% | -0.30% | 0.14% | 0.566 |
| CAR (-2, 2) | -1.04% | -0.17% | 0.87% | 0.016 |
| CAR (-3, 3) | -1.14% | -0.31% | 0.83% | 0.039 |

Panel C: Independent variables

| | Full Sample | | | | |
|---|---|---|---|---|---|
| Variable | Mean | Std Dev | Q1 | Median | Q3 |
| SIZE | 9.892 | 2.259 | 8.234 | 9.932 | 11.639 |
| ROA | 0.056 | 0.265 | 0.012 | 0.039 | 0.074 |
| OCF | 0.088 | 0.083 | 0.027 | 0.082 | 0.131 |
| LEV | 0.673 | 0.268 | 0.516 | 0.659 | 0.873 |
| FIN | -0.008 | 0.122 | -0.045 | -0.009 | 0.010 |
| PRIOR | 0.519 | 0.500 | 0.000 | 1.000 | 1.000 |
| CSR | 0.499 | 0.311 | 0.222 | 0.556 | 0.778 |
| Severity Quantitative | 0.139 | 0.665 | 0.000 | 0.000 | 0.005 |
| Severity Qualitative | 0.226 | 0.418 | 0.000 | 0.000 | 0.000 |
| Locus Internal | 0.147 | 0.354 | 0.000 | 0.000 | 0.000 |
| Controllability | 0.234 | 0.424 | 0.000 | 0.000 | 0.000 |
| CEO Ownership | 0.520 | 2.954 | 0.000 | 0.000 | 0.051 |

Table 3 reports the correlations of the variables. *CAR* is positively correlated with *SIZE* (correlation = 0.08) and *CSR* (correlation = 0.08), indicating less negative market reactions to data breaches by larger firms and firms with better CSR performance. Importantly, *CAR* is negatively correlated with *Severity Quantitative* (correlation = -0.17), *Severity Qualitative* (correlation = -0.12), and *Controllability* (correlation = -0.07), providing preliminary, univariate support for $H_1$ and $H_3$. While the correlation between *CAR* and *CEO ownership* is positive, it is not significant at the 0.10 level. The correlations among the screening variables (i.e., *Severity Quantitative*, *Severity Qualitative*, *Locus Internal*, *Controllability*, and *CEO Ownership*) are generally not significant, except that *Severity Quantitative* is positively correlated with

*CEO Ownership* (correlation = .08). In addition, the screening variables exhibit relatively low correlations with the control variables.

**Table 3. Correlation Table**

| Variables | CAR | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SIZE (1) | 0.08* | | | | | | | | | | | |
| ROA (2) | 0.03 | -0.08* | | | | | | | | | | |
| OCF (3) | 0.04 | -0.29* | 0.22* | | | | | | | | | |
| LEV (4) | -0.03 | 0.34* | -0.06 | -0.40* | | | | | | | | |
| FIN (5) | -0.04 | -0.03 | -0.05 | -0.23* | 0.43* | | | | | | | |
| Prior (6) | 0.02 | 0.43* | -0.04 | -0.05 | 0.15* | -0.06 | | | | | | |
| CSR (7) | 0.08* | 0.41* | -0.00 | 0.02 | 0.02 | -0.14* | 0.20* | | | | | |
| Severity Quantitative (8) | -0.17* | 0.05 | 0.00 | 0.04 | -0.05 | 0.02 | 0.06 | -0.03 | | | | |
| Severity Qualitative (9) | -0.12* | 0.07 | -0.06 | -0.16* | 0.07* | -0.02 | 0.05 | 0.08* | 0.04 | | | |
| Locus Internal (10) | 0.01 | 0.09* | -0.01 | 0.04 | 0.01 | 0.01 | 0.10* | 0.05 | -0.04 | 0.05 | | |
| Controllability (11) | -0.07* | 0.08* | -0.04 | -0.04 | 0.09* | 0.01 | 0.06 | 0.03 | 0.05 | -0.05 | -0.06 | |
| CEO Ownership (12) | 0.06 | -0.11* | -0.01 | 0.06 | -0.10* | 0.02 | -0.02 | -0.08* | 0.08* | -0.05 | -0.05 | -0.01 |

Note: * indicates the significance of the coefficients at or below the 10 percent level.

## 6.2 Multivariate Analysis of Market Reaction to Data Breaches

To test our hypotheses, we use the following multivariate regression model, which incorporates control variables, three breach characteristic variables, CEO ownership, CSR, and the interaction effects between breach characteristics, CEO ownership, and CSR.

$$\begin{aligned} CAR_t = {} & \beta_0 + \beta_1 SIZE_{t-1} + \beta_2 ROA_{t-1} + \beta_3 OCF_{t-1} + \beta_4 LEV_{t-1} + \beta_5 FIN_{t-1} + \beta_6 PRIOR_{t-1} \\ & + \beta_7 CSR_{t-1} + \beta_8 Severity\ Quantitative_t + \beta_9 * Severity\ Qualitative_t \\ & + \beta_{10} Locus\ Internal_t + \beta_{11} Controllability_t + \beta_{12} CEO\ Ownership_{t-1} \\ & + \beta_{13} CSR_{t-1} * Severity\ Quantitative_t + \beta_{14} CSR_{t-1} * Severity\ Qualitative_t \\ & + \beta_{15} CSR_{t-1} * Locus\ Internal_t + \beta_{16}\ CSR_{t-1} * Controllability_t \\ & + \beta_{17} CSR_{t-1} * CEO\ Ownership_{t-1} + Industry\ and\ Year\ Effects + \varepsilon_t \end{aligned} \quad (4)$$

$CAR_t$ is the cumulative abnormal return from 3 days before to 3 days after the breach announcement in year *t*. All the control variables, *CEO Ownership*, and *CSR* are measured at year t-1. Breach severity (*Severity Quantitative* and *Severity Qualitative*), *Locus Internal*, and *Controllability* are measured at year t when the data breach occurred.

Table 4 reports the results of the multivariate regression models with *CAR* ( -3, 3) as the dependent variable. Column I reports the regression results based on the control variables only; none of the control variables are significant. Column II reports the regression results of the model that includes the main effects of the breach characteristics, CEO ownership, and CSR performance on abnormal stock returns. We find that both *Severity Quantitative* (b = -.006, p < .05) and *Severity Qualitative* (b = -.011, p < .05) have a negative impact on abnormal stock returns, thus supporting $H_1$. Data breaches that involve a larger number of compromised records and that involve sensitive financial data incur more negative abnormal returns and thus a greater decline in the market value of the breached firm. *Locus Internal* is not significant (b = .0001, NS), implying that the stock market reaction is unaffected by whether the locus is internal or external to the firm. Therefore, $H_2$ is not supported. Consistent with $H_3$, *Controllability* (b = -.010, p < .05) has a negative effect on abnormal stock returns, suggesting that data breaches that are controllable incur more negative abnormal returns as compared to those that are not controllable. Further, the coefficient on *CEO Ownership* (b = .001, p < .05) is positive, providing support for $H_4$ that lower CEO stock ownership is associated with more negative abnormal returns (and higher CEO stock ownership is associated with less negative abnormal returns). Overall, the results reported in Column II indicate that the cumulative abnormal returns around breach announcements are negatively associated with severity and controllability and positively associated with CEO ownership (i.e., negatively associated with low CEO ownership), consistent with the view that these breach characteristics and corporate governance attributes may act as screens to drive the heterogeneous stock market reaction to data breaches. In contrast, breach locus does not have a significant impact on the abnormal returns of the breached firm, suggesting that the market does not differentiate between breaches with internal versus external locus of causality.

Column III presents the results based on the full model (4), with the control variables, the main effects of breach characteristics, CEO ownership, and CSR, as well as the interactive effects between breach characteristics, CEO ownership, and CSR. To test $H_5$, we examine the coefficients of relevant interaction terms in Column III. $H_{5a}$ hypothesizes that the effect of breach severity on abnormal returns will be less negative when CSR is high. We find a positive interaction between *CSR* and *Severity Quantitative* (b = .035, p < .01), which, coupled with the negative main effect of *Severity Quantitative* (b = -.022, p < .01), suggests that the negative effect of *Severity Quantitative* becomes smaller as CSR increases. Similarly, the positive interaction between *CSR* and *Severity Qualitative* (b = .041, p < .01), coupled with the negative main effect of *Severity Qualitative* (b = -.032, p < .01), suggests that the negative effect of *Severity Qualitative* becomes smaller as CSR increases. Thus, $H_{5a}$ is supported.

Neither the main effect of *Locus* (b = .007, NS) nor the interactive effect of *CSR x Locus* (b = -.016, NS) is significant, suggesting that CSR does not moderate the effect of Breach Locus. Therefore, $H_{5b}$ is not supported. For $H_{5c}$, there is a negative main effect of *Controllability* (b = -.027, p < .01) and a positive interaction between *CSR* and *Controllability* (b = .033, p < .05), suggesting that the negative effect of breach controllability decreases as CSR performance gets higher. Thus, $H_{5c}$ is supported.

To test $H_{5d}$, we examine the coefficients of *CEO Ownership* and *CSR x CEO Ownership*. The coefficient on *CEO Ownership* (b = .004, p < .01) is positive and the coefficient on *CSR x CEO Ownership* (b = -.006, p <.01) is negative, suggesting that lower CEO Ownership is associated with more negative abnormal returns (i.e., high CEO ownership, as indicator of better corporate governance, has a positive effect on abnormal return) and, as CSR performance increases, the negative effect of low CEO ownership (or the positive effect of high CEO ownership) becomes smaller. The results suggest that CSR attenuates the negative effect of low CEO ownership on the cumulative abnormal returns, supporting $H_{5d}$.

**Table 4. Multivariate Analysis of Market Reaction to Data Breach**

| | Dependent Variable = CAR (-3, +3) | | | | | |
|---|---|---|---|---|---|---|
| | I | | II | | III | |
| | Coeff. | t-stat | Coeff. | t-stat | Coeff. | t-stat |
| SIZE | 0.001 | (1.10) | 0.001 | (0.39) | 0.001 | (0.92) |
| ROA | -0.003 | (-0.42) | -0.003 | (-0.42) | -0.006 | (-0.75) |
| OCF | 0.001 | (0.04) | -0.024 | (-0.76) | -0.014 | (-0.46) |
| LEV | -0.009 | (-0.89) | -0.005 | (-0.57) | -0.007 | (-0.70) |
| FIN | 0.001 | (0.07) | -0.007 | (-0.40) | -0.006 | (-0.35) |
| PRIOR | -0.001 | (-0.12) | 0.002 | (0.41) | 0.000 | (0.01) |
| CSR | | | 0.006 | (0.83) | -0.012 | (-1.43) |
| Severity Quantitative | | | -0.006 | (-1.97)** | -0.022 | (-3.37)*** |
| Severity Qualitative | | | -0.011 | (-2.40)** | -0.032 | (-3.24)*** |
| Locus Internal | | | 0.001 | (0.23) | 0.007 | (0.66) |
| Controllability | | | -0.010 | (-2.32)** | -0.027 | (-2.94)*** |
| CEO Ownership | | | 0.001 | (2.26)** | 0.004 | (3.66)*** |
| CSR x Severity Quantitative | | | | | 0.035 | (3.29)*** |
| CSR x Severity Qualitative | | | | | 0.041 | (2.82)*** |
| CSR x Locus Internal | | | | | -0.016 | (-0.95) |
| CSR x Controllability | | | | | 0.033 | (2.33)** |
| CSR x CEO Ownership | | | | | -0.006 | (-2.81)*** |
| Industry and Year Effects | Yes | | Yes | | Yes | |
| Adjusted $R^2$ | 0.009 | | 0.041 | | 0.089 | |
| Number of Observations | 607 | | | | | |
| Note: *, **, or *** indicate significance at the 10%, 5%, or 1% level, respectively. | | | | | | |

In sum, we find empirical support for $H_{5a}$, $H_{5c}$, and $H_{5d}$ that CSR performance mitigates the negative impacts of breach severity, breach controllability, and low CEO ownership on the market reaction to breach announcements. In addition, the explanatory power of the model (i.e., $R^2$ 8.9%) is higher than, or comparable to, that documented in prior studies on the market reaction to data breaches (e.g., Gwebu, Wang, and Wang 2018; Martin et al. 2017; Rasoulian et al. 2021).

## 6.3 Robustness Analysis

We conduct several additional tests to assess the robustness of our findings. First, we add a sequence of dummy variables ($DUM_1$, $DUM_2$ … $DUM_n$) into model (4) to control for the sequential effects of breach incidents. In particular, $DUM_i$ (i = 1, 2…n) is equal to 1 for the ith announcement subsequent to the first

announcement for a firm and zero otherwise. The results are reported in Column I of Table 5 and are qualitatively similar to those in Column III of Table 4. In addition, none of the sequential effects (untabulated) is associated with the market reaction to breach announcements. This is consistent with the insignificant effect of *PIROR* on the cumulative abnormal returns as reported in Table 4.

Second, in our main analysis, we control for industry and year fixed effects. This is in line with prior research on event studies (e.g., Rasoulian et al. 2021; Martin et al. 2017) and follows the recommendation of Gormley and Matsa (2014), who cautioned against using fixed firm effects when there is little within-firm variation in the variables of interest. As a robustness test, we replace industry fixed effects in model (4) with firm fixed effects to control for unobservable firm characteristics that may affect the market reaction to breach announcements. We report the results in Column II of Table 5. Our main findings are robust to the inclusion of firm fixed effects, except that the coefficients on both *Severity Qualitative* and *CSR x Severity Qualitative* become insignificant. We note that the *Severity Qualitative* measure is mostly time-invariant within a firm, because whether the breached data contains financial information is likely to be highly correlated with the nature and scope of a firm's business activities. Not surprisingly, its explanatory power for the cumulative abnormal returns is subsumed by fixed firm effects. In addition, adding firm fixed effects significantly increases the $R^2$ from 0.089 to 0.520.

Third, since our main analysis uses market-adjusted abnormal returns as the dependent variable, we test the robustness of our results by using the Fama-French three-factor model to recalculate the cumulative abnormal returns (CAR) during the event window. The Fama-French model takes into account market return, firm size, and the book-to-market ratio when estimating abnormal returns (Fama and French 1993). The multivariate analysis of market reaction to a data breach based on the three-factor Fama-French model produces qualitatively similar results as those documented in Table 4. In addition, since our main analysis uses the decile ranks of CSR scores, to check whether our results are robust to alternative ways of ranking CSR, we use the quintile ranks of CSR scores to measure CSR performance. Using the quintile ranks of CSR scores yields qualitatively similar results as those reported in Table 4.

**Table 5. Controlling for Sequential Effects and Fixed Firm Effects**

| | Dependent Variable = CAR (-3, +3) | | | |
|---|---|---|---|---|
| | I | | II | |
| | Coeff. | t-stat | Coeff. | t-stat |
| SIZE | 0.001 | (1.00) | -0.024 | (-2.22)** |
| ROA | -0.005 | (-0.70) | -0.011 | (-1.24) |
| OCF | -0.012 | (-0.38) | -0.101 | (-1.65)* |
| LEV | -0.006 | (-0.67) | -0.067 | (-2.06)** |
| FIN | -0.005 | (-0.31) | -0.034 | (-0.87) |
| PRIOR | -0.011 | (-0.83) | -0.008 | (-1.62) |
| CSR | -0.013 | (-1.43) | -0.003 | (-0.21) |
| Severity Quantitative | -0.020 | (-2.76)*** | -0.026 | (-3.69)*** |
| Severity Qualitative | -0.035 | (-3.43)*** | -0.001 | (-0.10) |
| Locus Internal | 0.008 | (0.72) | 0.011 | (0.82) |
| Controllability | -0.028 | (-2.93)*** | -0.031 | (-2.59)** |
| CEO Ownership | 0.004 | (3.64)*** | 0.003 | (2.38)** |
| CSR x Severity Quantitative | 0.030 | (2.64)*** | 0.040 | (3.63)*** |
| CSR x Severity Qualitative | 0.044 | (2.98)*** | -0.001 | (-0.04) |
| CSR x Locus Internal | -0.017 | (-1.00) | -0.015 | (-0.85) |
| CSR x Controllability | 0.034 | (2.32)** | 0.034 | (2.00)** |
| CSR x CEO Ownership | -0.006 | (-2.81)*** | -0.023 | (-2.59)** |
| Year Effects | Yes | | Yes | |
| Industry Effects | Yes | | No | |
| Firm Effects | No | | Yes | |
| Sequential Effects | Yes | | No | |
| Adjusted $R^2$ | 0.076 | | 0.520 | |
| Number of Observations | 607 | | | |
| Note: *, **, or *** indicate significance at the 10%, 5%, or 1% level, respectively. | | | | |

Fourth, prior research suggests that the qualitative aspect of breach severity is related to whether the breached information is financial or whether it is personal/medical (Malhotra and Malhotra 2011; Rasoulian et al. 2021). We examine the impact of breached financial information as the qualitative aspect of breach severity in our main analysis. As an additional analysis, we use an alternative measure of

*Severity Qualitative* by looking at whether the data breaches involve personal/medical information. Specifically, we code *Severity Qualitative* as 1 if the breach announcement contains key words such as social security number/SSN, driver's license number, birthday, date of birth (DOB), passport, medical/MED, and 0 otherwise. Using this alternative measure of *Severity Qualitative*, we find that the coefficients on *Severity Qualitative* and *CSR* × *Severity Qualitative* are not significant. This suggests that whether or not a data breach involves personal/medical information does not have a significant impact on stock market reaction. Such nonsignificant effect of personal/medical information is in line with prior research; Rasoulian et al. (2021) find that the impact of personal/medical information on stock market reaction is weak or inconsistent.

Finally, one could argue that a firm's past breach history may act as an additional screen: firms with prior breaches might be perceived as having weak data security management capabilities and thus higher data breach risks. To test this, we examine the coefficient of *PRIOR* and add *CSR* × *PRIOR* as an additional variable in Model (4). We find that neither *PRIOR* nor *CSR* × *PRIOR* has a significant coefficient, indicating that a firm's historical record of breaches does not have a significant main effect on stock market reaction, and that CSR performance does not moderate the effect of the prior breach record.

## 6.4 Additional Analysis on Longer-Term Market Reaction to Data Breaches

To get a longer and more comprehensive view of the stock market reaction to data breach, we conducted additional analysis to examine subsequent stock market trends of the breached firms following the (-3,3) event window. More specifically, we examined how CAR for time windows (4, 14), (15, 29), and (30-60), respectively, are influenced by our model. Examining the market reaction after the (-3, 3) event window allowed us to understand whether the market overreacts or underreacts to our screening variables. If investors underreact to the screening variables during the (-3, 3) event window, the market should continue to react to these variables after the event period in a similar way to those documented in Table 4. In contrast, if investors overreact to the screening variables, the stock price reaction during the event window should revert, suggesting that the associations between the abnormal returns following the event period and the screening variables should be opposite to those shown in Table 4.

Table 6 reports the longer-term market reaction to our screening variables following the event window. The results for CAR (4, 14) in Column I indicate that the market underreacts during the (-3, 3) event window to *Severity Quantitative* and *CEO Ownership*, as evidenced by the negative coefficient on *Severity Quantitative* (b = -.014, p < .10) and the positive coefficient on *CSR x Severity Quantitative* (b = .022, p < .10), the positive coefficient of CEO Ownership (b = .007, p < .01) and the negative coefficient of CSR x CEO Ownership (b = -.008, p < .01). On the other hand, the results for CAR (4, 14) in Column 1 indicate that the market overreacts to *Controllability* during the (-3, 3) window, as evidenced by a positive coefficient on *Controllability* (b = .028, p < .05) and a negative coefficient on *CSR x Controllability* (b = -.035, p < .10). We continue to find an underreaction to *Severity Quantitative* during the window (15, 29), as evidenced by the negative coefficient on *Severity Quantitative* (b = -.026, p < .01) and the positive coefficient on *CSR x Severity Quantitative* (b = .037, p < .05) in Column II. In contrast, the cumulative abnormal returns during the window (30, 60) are not associated with any of our screening variables in Column III, suggesting that the market has fully digested the implications of the information contained in breach announcements for firm value 30 days after breach announcements.

**Table 6. Longer-term Market Reaction to Data Breaches**

| | Dependent Variable = CAR | | | | | |
|---|---|---|---|---|---|---|
| | CAR (4,14)<br>I | | CAR (15,29)<br>II | | CAR (30,60)<br>III | |
| | Coeff. | t-stat | Coeff. | t-stat | Coeff. | t-stat |
| SIZE | 0.001 | (0.44) | 0.000 | (0.10) | 0.008 | (2.70)*** |
| ROA | 0.010 | (1.05) | 0.009 | (0.77) | 0.007 | (0.38) |
| OCF | 0.066 | (1.90)* | -0.010 | (-0.23) | 0.087 | (1.34) |
| LEV | -0.006 | (-0.53) | -0.016 | (-1.11) | -0.020 | (-0.95) |
| FIN | 0.043 | (2.02)** | 0.044 | (1.65)* | 0.008 | (0.20) |
| PRIOR | -0.005 | (-1.00) | 0.005 | (0.80) | -0.005 | (-0.52) |
| CSR | 0.019 | (1.73)* | 0.012 | (0.92) | -0.011 | (-0.57) |
| Severity Quantitative | -0.014 | (-1.95)* | -0.026 | (-2.98)*** | 0.005 | (0.38) |
| Severity Qualitative | 0.006 | (0.51) | 0.007 | (0.44) | 0.012 | (0.52) |
| Locus Internal | 0.019 | (1.41) | 0.005 | (0.31) | 0.007 | (0.26) |
| Controllability | 0.028 | (2.37)** | -0.007 | (-0.50) | -0.014 | (-0.62) |

| | | | | | | |
|---|---|---|---|---|---|---|
| CEO Ownership | 0.007 | (4.63)*** | -0.001 | (-0.38) | 0.004 | (1.33) |
| CSR x Severity Quantitative | 0.022 | (1.85)* | 0.037 | (2.56)** | 0.005 | (0.23) |
| CSR x Severity Qualitative | 0.001 | (0.07) | -0.003 | (-0.13) | -0.010 | (-0.29) |
| CSR x Locus Internal | -0.024 | (-1.15) | -0.018 | (-0.70) | -0.034 | (-0.90) |
| CSR x Controllability | -0.035 | (-1.96)* | 0.015 | (0.70) | 0.011 | (0.34) |
| CSR x CEO Ownership | -0.008 | (-2.90)*** | 0.002 | (0.57) | -0.004 | (-0.73) |
| Year Effects | Yes | | Yes | | Yes | |
| Industry Effects | Yes | | Yes | | Yes | |
| Adjusted $R^2$ | 0.088 | | 0.008 | | 0.021 | |
| No. of Obs. | 607 | | | | | |
| Note: *, **, or *** indicate significance at the 10%, 5%, or 1% level, respectively. | | | | | | |

Prior research (e.g., Barber and Lyon 1997) argues that, for long-horizon event study, buy and hold abnormal returns are more suitable than cumulative abnormal returns. We thus examine the buy-and-hold monthly abnormal returns starting from the beginning of 2 months after the month when breach announcements were made. We regression buy and hold abnormal returns from month 2 to month 4, 7, and 13, respectively, on our model to examine the effects of our screening variables; untablulated results show that there is no significant association between long-run stock returns and any of our screening variables. The results are consistent with those documented in Column III of Table 6 and suggest that there is no mispricing of our screening variables from 2 months after the event month.

# 7 Discussion

Given the substantial heterogeneity in the impact of data breach incidents on firm value (Gatzlaff & McCullough, 2010; Malhotra & Kubowicz Malhotra, 2011; Rasoulian et al., 2021), this study seeks to deepen our current understanding of the breach- and firm-related factors that influence the stock market reaction to a data breach. Drawing upon the screening theory (Connelly et al., 2011; Spence, 1978), we identify three breach characteristics (severity, locus, and controllability) and two firm attributes (CEO stock ownership and CSR performance) that may serve as screens to impact the stock market's reaction to data breaches. Providing support for our hypotheses, the results show that the stock market reacts more negatively when a data breach incident is more severe or controllable, or when the breached firm has a low proportion of CEO stock ownership. Further, CSR acts as an insurance policy by mitigating the negative impacts of severity, controllability, and low CEO ownership on firm value. Overall, these significant results pinpoint the contextual dependence of stock market reaction to data breaches on key breach-level and firm-level characteristics.

## 7.1 Theoretical Implications

This research contributes to data breach literature on multiple fronts. First, a conceptual foundation of how the contextual characteristics of a breach impact market reaction is currently lacking. Using a relatively unique theoretical perspective known as screening theory (Connelly et al., 2011; Spence, 1978), this research offers insight into how the stock market may react to a data breach announcement in the presence of information scarcity and asymmetry. The screening theory provides a promising framework for integrating an array of contextual factors, identified from distinct streams of research, under one common umbrella. Given the relative lack of integrative efforts in the literature analyzing the financial consequences of data breaches, we consider this study's integrative approach to be a significant theoretical contribution. It offers rich, unified, and more coherent insights into the concomitant effects of the breach- and firm-level characteristics and discovers the conditions under which a breach is more or less consequential to the focal firm. The findings of this research provide empirical support for this integrative approach because multiple contextual factors have been found to drive the cross-sectional variations in the stock market's reaction to data breaches. The incorporation of a wide range of contextual variables also alleviates omitted variable bias, a potential issue that existed in prior research. Further, although their impacts on shareholder value have been well documented in other fields, CEO stock ownership and CSR performance have yet to be synthesized into the data breach literature. This study extends prior research by documenting the influences of CEO stock ownership and CSR record on firm value following a breach announcement.

Further, this study adds to the literature at the intersection of CSR and corporate crisis (Godfrey et al., 2009b; Klein & Dawar, 2004) by documenting the insurance-like effect of CSR in the data breach context. Specifically, we show that CSR helps a firm preserve its economic value by mitigating the negative effects

of severity, controllability, and low CEO ownership. Research on data breaches has only recently begun to explore mechanisms that are effective in helping firms weather the adverse impact of a breach (Gwebu et al., 2018). This study helps expand the scope of current data breach research to include breach damage control and recovery by highlighting the critical role of CSR in reducing adverse market reaction to a data breach.

Our study extends the screening theory to a new context (i.e., data breaches) and opens a promising avenue for future research. The screening theory provides a robust theoretical lens to understand which information elements may act as screens, guiding shareholders' investment decisions and reducing information asymmetry. While our focus is on data breaches, the concept of screens can be extended to a diverse range of other corporate crisis situations.

## 7.2 Practical Implications

This study explores both the immediate and longer-term impacts of breach characteristics and CEO ownership on firm value. These findings hold substantial significance for both investors and firms. From an investor's perspective, the market's propensity to overreact to controllability and underreact to severity presents short-term trading opportunities for those closely monitoring stock prices in the aftermath of a breach. Nevertheless, beyond the initial 30 days, the market effectively incorporates breach-related information, reducing trading opportunities for long-term investors.

From a firm’s perspective, corporate executives and managers have a large stake in better understanding the economic impacts of various contextual characteristics surrounding a breach. Past studies consistently demonstrate that internal causal locus, as opposed to external causal locus, tends to have a more adverse impact on stakeholder perceptions, satisfaction, and behavioral responses across a diverse array of crisis contexts (Folkes, 1984; Munyon, Jenkins, Crook, Edwards, & Harvey, 2019; Vaidyanathan, & Aggarwal, 2003). Accordingly, firms, often constrained by limited resources, may be tempted to prioritize resource allocation and capability building to prevent internally caused breaches while potentially neglecting other breach types. However, the findings from this research suggest the necessity of adopting a more nuanced approach. Specifically, our results show that, on average, stakeholders do not differentiate between breaches with internal or external locus of causality. This result suggests that an external partner's weak capability, lack of best practices, or inadequate standard in information security management can pose significant risks for the focal firm. Hence, it becomes crucial for companies not only to implement robust security controls and measures internally but also to develop a deeper understanding of their external partners' information security management and practices to safeguard themselves from potential spillover liability from breaches caused by external partners. Firms may also consider adopting a risk-sharing strategy, wherein the responsibility and accountability for safeguarding the firm's information assets are shared with external partners through contractual agreements.

On the other hand, our research finds that severe breaches (involving more records and sensitive financial data) lead to more adverse market reactions. Additionally, the market underreacts to Severity Quantitative (i.e., the quantity of breached records), indicating a prolonged and underestimated impact of Severity Quantitative on firm value. In light of these findings, firms not only must rigorously safeguard their data repositories, especially those housing a large amount of sensitive financial information, they must also reassess risk tolerance and integrate potential longer-term stock price effects into risk management and financial planning.

Although the research indicates that investors initially react more negatively to breaches perceived as controllable (i.e., could have been avoided), the additional analyses reveal a market overreaction to controllability during the (-3,3) event window, with the effect later reverting. This suggests that, with time, investors may discount the informativeness of controllability and play less weight on breach controllability as an information screen. Therefore, while firms should undoubtedly work to minimize breaches that are reasonably controllable by instituting necessary data security infrastructure, strictly implementing responsible data policies and processes, and investing sufficient resources for routine maintenance and upgrade (Densham, 2015), they must also recognize the importance of strengthening their capabilities to mitigate breaches that are less controllable by proactively identifying emerging threats, enhancing incident response plans, and collaborating with cybersecurity experts to develop advanced threat detection and mitigation strategies. This dual approach is crucial for maintaining investor confidence.

Finally, our results suggest that firms should implement better corporate governance by increasing the weight of equity-based compensation (e.g., stocks) in CEO compensation to incentivize long-term oriented

behavior (e.g., proactively managing a firm's cybersecurity challenges). Data breaches are oftentimes unavoidable despite a firm's best efforts. Thus, it is important to understand what factors could mitigate the negative effects of a data breach. Our findings suggest that, by investing in CSR activities and building a high stock of CSR-based moral capital, firms could be insulated, to a certain extent, from the negative economic consequences of a data breach. Thus, managers should strengthen their firm's CSR performance to reap the benefits of the insurance-like protection afforded by CSR when a data breach does occur.

Additionally, our research also suggests that firms could engage in timely post-breach communication to shape stakeholders' interpretation and cognitive sense-making of the breach by proactively signaling the characteristics of a breach (i.e., severity, locus, and controllability) as well as firm attributes such as CEO stock ownership and favorable CSR performance. On the other hand, however, unscrupulous firms could mislead stakeholders into misevaluating a breach by giving pretentious reasons. Thus, stakeholders and policymakers need to be cognizant of firms that may use post-breach communication unethically to manipulate public opinion and stock market responses.

# 8 Limitations and Future Research

The results presented in this study have some limitations, many of which may be addressed by future studies. First, this research only considers breach characteristics disclosed in the breach announcement. Future studies may examine the possibility of other information cues from the announcement serving as screens to drive the cross-sectional variations in stock market reaction to a data breach. Second, this research focuses on the impact of various information screens on the stock market's reaction to data breaches. Information screens that are effective for one stakeholder group may not be equally effective for another group. Thus, one logical extension is for scholars to theorize and compare the effectiveness of various information screens when different stakeholder groups are considered. Finally, it is also important to note that our framework is applicable beyond the contextual factors included in this study; the screening theory can flexibly incorporate other breach characteristics.

## References


Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings* (p. 94).

Antonetti, P., & Maklan, S. (2016). An extended model of moral outrage at corporate social irresponsibility. *Journal of Business Ethics*, *135*(3), 429–444.

Barber, B. M., & Lyon, J. D. (1997). Detecting long-run abnormal stock returns: The empirical power and specification of test statistics. *Journal of financial economics*, *43*(3), 341-372.

Barclay, L. J., Skarlicki, D. P., & Pugh, S. D. (2005). Exploring the role of emotions in injustice perceptions and retaliation. *Journal of Applied Psychology*, *90*(4), 629.

Bergami, M., & Bagozzi, R. P. (2000). Self-categorization, affective commitment and group self-esteem as distinct aspects of social identity in the organization. *British Journal of Social Psychology*, *39*(4), 555–577.

Bergh, D. D., Peruffo, E., Chiu, W. T., Connelly, B., & Hitt, M. A. (2020). Market response to divestiture announcements: A screening theory perspective. Strategic Organization, 18(4.

Bhagat, S., Brickley, J. A., & Lease, R. C. (1985). Incentive effects of stock purchase plans. *Journal of Financial Economics*, *14*(2), 195–215.

Bhagwat, Y., Warren, N. L., Beck, J. T., & Watson, G. F. (2020). Corporate sociopolitical activism and firm value. *Journal of Marketing*, *84*(5), 1–21.

Bhattacharya, C. B., & Sen, S. (2003). Consumer-company identification: A framework for understanding consumers' relationships with companies. *Journal of Marketing*, *67*(2), 76–88.

Bolton, L. E., & Mattila, A. S. (2015). How does corporate social responsibility affect consumer response to service failure in buyer–seller relationships? *Journal of Retailing*, *91*(1), 140–153.

Brown, K. C., & Harlow, W. V. (1988). Market overreaction. *Magnitude and intensity. Journal of Portfolio*, *14*(2), 6–13.

Chatterjee, S., Gao, X., Sarkar, S., & Uzmanoglu, C. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research*, *101*, 183–193.

Cohen, J. (1960), A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*. 20, (1), 37–46.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, 37(1), 39-67.

Connelly, B. L., Shi, W., Cheng, X., & Yin, C. (2021). Short Sellers: A screening theory perspective on B2B relationships. Journal of Business Research, 134.

Coombs, W. T. (1998). An analytic framework for crisis situations: Better responses from a better understanding of the situation. Journal of public relations.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS quarterly*, 673–687.

Currim, I. S., Lim, J., & Kim, J. W. (2012). You get what you pay for: the effect of top executives' compensation on advertising and R&D spending decisions and stock market return. *Journal of Marketing*, *76*(5), 33–48.

Dawar, N., & Pillutla, M. M. (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. *Journal of Marketing Research*, *37*(2), 215–226.

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5–8.

Du, S., Bhattacharya, C. B., & Sen, S. (2007). Reaping relational rewards from corporate social responsibility: The role of competitive positioning. *International journal of research in marketing*, *24*(3), 224–241.

Du, S., Bhattacharya, C. B., & Sen, S. (2011). Corporate social responsibility and competitive advantage: Overcoming the trust barrier. *Management Science*, *57*(9), 1528–1545.

Du, S., Yu, K., Bhattacharya, C. B., & Sen, S. (2017). The business case for sustainability reporting: Evidence from stock market reactions. *Journal of Public Policy & Marketing*, *36*(2), 313–330.

Folkes, V. S. (1984). Consumer reactions to product failure: An attributional approach. *Journal of Consumer Research*, *10*(4), 398–409.

Folkes, V. S., Koletsky, S., & Graham, J. L. (1987). A field study of causal inferences and consumer reaction: the view from the airport. *Journal of consumer research*, *13*(4), 534–539.

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

Gerstner, C. R., & Day, D. V. 1997. Meta-analytic review of leader-member exchange theory: Correlates and construct issues. *Journal of Applied Psychology*, 82(1), 827-844.

Gino, F., Shu, L. L., & Bazerman, M. H. (2010). Nameless+ harmless= blameless: When seemingly irrelevant factors influence judgment of (un) ethical behavior. *Organizational Behavior and Human Decision Processes*, *111*(2), 93–101.

Godfrey, P. C. (2005). The relationship between corporate philanthropy and shareholder wealth: A risk management perspective. *Academy of management review*, *30*(4), 777–798.

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009a). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management*, *Journal,30(4*, 425–445.

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009b). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management*, *Journal,30(4*, 425–445.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410.

Gormley, T. A., & Matsa, D. A. (2014). Common errors: How to (and not to) control for unobserved heterogeneity. *The Review of Financial Studies*, *27*(2), 617–661.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems*, *35*(2), 683–714.

Hamilton, V. L. (1980). Intuitive psychologist or intuitive lawyer? Alternative models of the attribution process. *Journal of Personality and Social Psychology*, *39*(5), 767.

Hartmann, J., & Moeller, S. (2014). Chain liability in multitier supply chains? Responsibility attributions for unsustainable supplier behavior. *Journal of Operations Management*, *32*(5), 281–294.

IBM. (2021). Cost of A Data Breach Report 2021.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of financial economics*, *3*(4), 305–360.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, *45*(2), 208–228.

Kelley, H. H., & Michela, J. L. (1980). Attribution theory and research. *Annual Review of Psychology*, *31*(1), 457–501.

Kervyn, N., Fiske, S. T., & Malone, C. (2012). Brands as intentional agents framework: How perceived intentions and ability can map brand perception. *Journal of Consumer Psychology*, *22*(2), 166– 176.

Klein, J., & Dawar, N. (2004). Corporate social responsibility and consumers' attributions and brand evaluations in a product–harm crisis. *International Journal of research in Marketing*, *21*(3), 203–217.

Kotler, P., & Lee, N. (2005). *Corporate social responsibility: Doing the most good for your company and your cause*. Hoboken, NJ: John Wiley and Sons.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies.

*Information & Management*, *41*(5), 597–607.

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, *135*, 559–571.

Landis, J.R. and Koch, G. G. (1977). The measurement of observer agreement for categorical data *Biometrics*. 33(1)159-174

Lange, D., & Washburn, N. T. (2012). Understanding attributions of corporate social irresponsibility.

*Academy of Management Review*, *37*(2), 300–326.

Laufer, D., Gillespie, K., McBride, B., & Gonzalez, S. (2005). The role of severity in consumer attributions of blame: Defensive attributions in product-harm crises in Mexico. *Journal of International Consumer Marketing*, *17*(2–3), 33–50.

Lenz, I., Wetzel, H. A., & Hammerschmidt, M. (2017). Can doing good lead to doing poorly? Firm value implications of CSR in the face of CSI. *Journal of the Academy of Marketing Science*, *45*(5), 677–697.

Luo, X., & Bhattacharya, C. B. (2009). The debate over doing good: Corporate social performance, strategic marketing levers, and firm-idiosyncratic risk. *Journal of marketing*, *73*(6), 198–213.

Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: an event study approach. *Journal of Service Research*, *14*(1), 44–59.

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

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155.

Mehran, H. (1995). Executive compensation structure, ownership, and firm performance. *Journal of financial economics*, *38*(2), 163–184.

Mudrack, P. E., & Mason, E. S. (2013). Ethical judgments: What do we know, where do we go? *Journal of Business Ethics*, *115*(3), 575–597.

Panagopoulos, N. G., Mullins, R., & Avramidis, P. (2018). Sales force downsizing and firm-idiosyncratic risk: The contingent role of investors' screening and firm's signaling processes. *Journal of Marketing*, *82*(6), 71-88.

Park, E., Kim, K. J., & Kwon, S. J. (2017). Corporate social responsibility as a determinant of consumer loyalty: An examination of ethical standard, satisfaction, and trust. *Journal of Business Research*, *76*, 8–13.

Qian, C., Crilly, D., Wang, K., & Wang, Z. (2021). Why do banks favor employee-friendly firms? A stakeholder-screening perspective. Organization Science, 32(3.

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2021). The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements.

*Journal of Service Research*.

Ridge, J. W., Ingram, A., Abdurakhmonov, M., & Hasija, D. (2019). Market reactions to non-market strategy: Congressional testimony as an indicator of firm political influence. *Strategic Management Journal*, *40*(10), 1644-1667.

Sanders, W. G., & Boivie, S. (2004). Sorting things out: Valuation of new firms in uncertain markets.

Strategic. *Management*, *25*(2), 167–186.

Scott, W. R. (1987). The adolescence of institutional theory. *Administrative Science Quarterly*, 493–511.

Sen, S., Du, S., & Bhattacharya, C. B. (2016). Corporate social responsibility: a consumer psychology perspective. *Current Opinion in Psychology*, *10*, 70–75.

Servaes, H., & Tamayo, A. (2013). The impact of corporate social responsibility on firm value: The role of customer awareness. *Management Science*, *59*(5), 1045–1061.

Spence, M. (1978). *Job market signaling. In Uncertainty in economics (pp*. Academic Press.

Statista. (2023). Annual number of data compromises and individuals impacted in the United States from 2005 to first half 2022.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610.

Surroca, J., Tribó, J. A., & Waddock, S. (2010). Corporate responsibility and financial performance: The role of intangible resources. *Strategic Management Journal*, *31*(5), 463–490.

Torres, A., Bijmolt, T. H., Tribó, J. A., & Verhoef, P. (2012). Generating global brand equity through corporate social responsibility to key stakeholders. *International Journal of Research in Marketing*, *29*(1), 13–24.

Turban, D. B., & Greening, D. W. (1997). Corporate social performance and organizational attractiveness to prospective employees. *Academy of Management Journal*, *40*(3), 658–672.

Vanhamme, J., & Grobben, B. (2009). Too good to be true!". The effectiveness of CSR history in countering negative publicity. *Journal of Business Ethics*, *85*, 273–283.

Vitell, S. J. (2003). Consumer ethics research: Review, synthesis and suggestions for the future. *Journal of Business Ethics*, *43*(1–2), 33–47.

Waddock, S. (2003). Myths and realities of social investing. *Organization & Environment*, *16*(3), 369–380.

Walsh, G., & Bartikowski, B. (2013). Exploring corporate ability and social responsibility associations as antecedents of customer satisfaction cross-culturally. *Journal of business research*, *66*(8), 989–995.

Weiner, B. (1980). A cognitive (attribution)-emotion-action model of motivated behavior: An analysis of judgments of help-giving. *Journal of Personality and Social Psychology*, *39*(2), 186.

Weiss, A. (1995). Human capital vs. *signalling explanations of wages. Journal of Economic*, *9*(4), 133–154.

Xie, C., Bagozzi, R. P., & Grønhaug, K. (2015). The role of moral emotions and individual differences in consumer responses to corporate green and non-green actions. *Journal of the Academy of Marketing Science*, *43*(3), 333–356.

Yermack, D. (1997). Good timing: CEO stock option awards and company news announcements. *The journal of Finance*, *52*(2), 449–476.

Zhang, Y., & Wiersema, M. F. (2009). Stock market reaction to CEO certification: The signaling role of CEO background. *Strategic Management Journal*, *30*(7), 693–710.

## About the Authors

**Shuili Du** is Professor of Marketing at the Peter T. Paul College of Business and Economics, University of New Hampshire. Her research focuses on corporate social responsibility (CSR) and stakeholder reactions, CSR communication, sustainability reporting, and sustainable product innovation. Her latest research focuses on the evolving role of CSR in the age of artificial intelligence. Dr. Du's research has appeared in the *Journal of Consumer Research, Management Science, International Journal of Research in Marketing, Journal of Public Policy and Marketing, Journal of Business Ethics, Journal of Business Research*, and others. She frequently presents her research in leading academic forums both nationally and internationally.

**Kholekile L. Gwebu** is an associate professor of decision sciences at the Peter T. Paul College of Business and Economics, University of New Hampshire. His research focuses on data security management, information privacy, and information technology adoption and use. His publications appear in *Journal of Strategic Information Systems, Decision Support Systems, and Information Society, Journal of Management Information Systems* among others.

**Jing Wang** is an associate professor of decision sciences at the Peter T. Paul College of Business and Economics, University of New Hampshire. Her research focuses on the areas of information technology (IT) outsourcing, open-source software, IT adoption and use, privacy, and data security. Her work has been published in *Journal of Management Information Systems, Decision Support Systems, Journal of Strategic Information Systems, Journal of Business Research*, and in the proceedings of national and international information systems conferences.

**Kun Yu** is an associate professor of accounting at the College of Management, University of Massachusetts Boston. His research focuses on the value relevance of financial and nonfinancial information, pension accounting, earnings management, corporate governance, and sustainability reporting. Dr. Yu's research has appeared in *The Accounting Review*, *Journal of Business Ethics*, *Journal of Corporate Finance*, *Accounting and Business Research*, *Accounting and Finance*, and *Journal of Public Policy and Marketing*, among others.