Cyber Risk Contagion and Corporate Response: The Spillover Effects of Data Breaches on Tourism Industry Peers

ABSTRACT

This study investigates how data breaches impact firm value and corporate behaviors for both tourism firms and their industry peers. Our results show that data breaches significantly diminish firm value, as evident by a negative market reaction of -1.9% to the announcement of data breach made by a tourism firm. Importantly, the negative market reactions extend to non-breached firms within the same sub-industry, especially for those in the restaurant and hotel sub-industries. Such spillover effects are not homogeneous and more pronounced in cases of customer information leakage and when sub-industries experience multiple breaches, but are attenuated for large firms. Further analysis shows that firms experiencing data breaches tend to respond by increasing cash holdings and reducing their dividend payouts post-breach. Sub-industry peers of the breached firms also increase cash holdings as a strategic response. Overall, the findings highlight the impact of cybersecurity threats on firm valuation and strategic responses in corporate policies that goes beyond the firms experiencing data breaches.

1. Introduction

The significant rise in data breaches has posed substantial financial risks to firms across industries.[1] The average cost of a data breach reaches $4.45 million in 2023, marking a 15.3% increase from 2020 (IBM, 2023). Recognizing the growing threat, firms have increasingly identified cyber risk as a major financial concern, ranking it among the top three business risks alongside geopolitical conflicts and macroeconomic volatility (PWC, 2023). The tourism industry, heavily reliant on digital platforms to enhance operational efficiency (Amaro and Duarte, 2015; Law et al., 2014), is particularly vulnerable, as data breaches not only result in significant financial losses but also damage the reputations of firms operating in this sector.[2]

The tourism industry has witnessed growing research on data breaches, primarily addressing the causes of breaches, such as employees' awareness of online crime risks (Boto-García, 2023) and cost-cutting in cybersecurity budgets (Bovsh et al., 2023), as well as post-breach service recovery efforts, including word-of-mouth (Gao et al., 2021)[3] and compensation effects (Wang et al., 2022a)[4]. However, research in this sector has largely overlooked the effects of data breaches on investor behavior and managerial decision-making aimed at mitigating data breaches impacts.

This study addresses this gap by focusing on tourism firms to investigate the market reaction to data breaches and the corporate strategies implemented to mitigate their financial

1 In 2022 alone, 1,802 data breaches were recorded—a 53% increase compared to 2018—impacting over 422 million individuals (Statista, 2022).
2 For example, Marriott disclosed in 2018 through an official statement that information of more than 500 million customers, including names, phone numbers, email addresses and credit card details, had been affected in an identified data breach, which results in a 100 million expense in the following one year to compensate affected customers and recover the system according to the firm CFO in an earning call.
3 They indicate that while in general, consumers are more likely to spread positive word-of-mouth when a company is perceived as competent, low error stability, and that the trend is more obvious with competent firms and firms with which customers have communal relationships.
4 They examine how different types of compensation affect customers' perceived fairness during data breach recovery in the hotel industry.

repercussions. Data breaches have a direct and negative impact on firm value in the tourism industry due to customer dissatisfaction and increased external risks. According to gossip theory, customers perceive data breaches as a violation of trust, leading to negative emotional and cognitive reactions, such as feelings of betrayal and diminished trust (Mills 2010; Richman and Leary 2009). These responses are impactful in the tourism industry (Migacz et al., 2018; Weber and Sparks, 2009), where customer trust is critical for spending and profitability (Janakiraman et al., 2018; Hewagama et al., 2019; Ho et al., 2020). Furthermore, data breaches result in litigation risks (Romanosky et al., 2014), which further reduce investor confidence.

Data breaches extend their impact beyond the directly affected firms, triggering spillover effects within the industry. However, whether a firm's data breach positively or negatively influences the stock market performance of its industry peers remains inconclusive. On one hand, data breaches perceived as systemic, industry-wide threats (Lang and Stulz, 1992; Paruchuri and Misangyi, 2015) are likely to diminish the value of industry competitors by signaling to investors an elevated cyberattack risk (Kamiya et al., 2021). Furthermore, strong competitive links among firms in highly competitive industries, such as tourism, also lead to negative spillover effects, as data breaches prompt customers to shift preferences away from closely associated competitors (Roehm and Tybout, 2006). On the other hand, when the breach reveals adverse information specific to the affected firm, competitors may benefit, as it underscores their relative advantages in future profitability (Lang and Stulz, 1992; Kamiya et al., 2021).

Our results show that data breaches have a negative and significant impact on the abnormal stock returns of affected firms. These findings remain consistent across robustness tests. Further analysis of stock market reactions within specific sub-industries shows that the hotel and restaurant sectors experience significant negative market returns, with abnormal returns of -3.6% and -3.3% in the hotel sub-industry, and -2.5% and -2.2% in the restaurant sub-industry respectively. Furthermore, we identify spillover effects within the tourism industry, as peer firms exhibit significant negative outcomes when firms in the hotel and restaurant sectors experience data breaches. Cross-sectional tests reveal that the contagion spillover effect is more pronounced when data breaches involve customer information leakage and repeated data breaches and is less pronounced when firms disclose affected data or when breached firms are larger in size.

In terms of corporate policy, we expect that tourism firms are compelled to increase cash holdings to secure future debt repayment capability, compensate customers to recover from service failures (Ho et al., 2020; Rasoulian et al., 2017), and prepare for heightened litigation risks (Romanosky et al., 2014). Peer firms within the same sub-industry face pressures to increase cash reserves, both to address operational income declines (Janakiraman et al., 2018; Hewagama et al., 2019) and to enhance internal controls for greater resilience against potential breaches (Ashraf, 2022; Wang et al., 2024). Thus, data breaches not only harm stock returns but also lead to increased cash holdings for both affected firms and their industry peers. Consistent with this notion, firms affected by data breaches hold 6% more cash relative to sales compared to non-breached years in the year following the breach, with these effects primarily driven by the hotel sub-industry. Additionally, breached firms reduce dividend payments by 15% compared to non-breached periods. Our findings also indicate that tourism peer firms tend to hold 3% more cash relative to sales in the year following the breach.

Our research contributes to the current literature in three ways. First, we are among the first to examine the impact of data breach events to the tourism industry. The current body of research predominantly focuses on the causes of data breaches, such as hospitality workers' awareness of online crime risks (Boto-García, 2023) and reductions in cybersecurity expenditures (Bovsh et al., 2023). Another stream of research investigates the impact of data breaches on customers under various service recovery strategies, including factors influencing customers' word-of-mouth behavior after data breaches in hotels (Gao et al., 2021), variations in customer reactions to compensation under different models (Wang et al., 2022a), and the effect of a firm's responsibility on customers' perceptions and revisit intentions following a data breach (Chen and Jai, 2019). However, the effects of data breaches on investor behavior and managerial decision-making aimed at mitigating these impacts remain underexplored. Our research provides critical evidence of the market reaction to data breaches among tourism firms and the role of corporate policies in mitigating their effects. This contribution expands the emerging literature on market reactions to data breaches.

Second, we are among the first to present evidence on how a firm’s actions affect its industry peers from the perspectives of investors and managers. Previous research in the tourism sector has primarily focused on spillover effects driven by customer actions. For example, studies have highlighted the positive spillover effect of increased bookings on adjacent rooms (Xu et al., 2022) and the spillover effect of satisfying stays on bookings for other properties owned by the same host (Xu et al., 2023). Other research has examined tourism spillovers from a spatial perspective, such as spatial spillovers within geographical clusters (Ma et al., 2015), across the top nine tourist destination countries in the EU (Mitra et al., 2019), and intra-industry spillover effects from foreign hotels to domestic ones in China (Mao and Yang, 2016). However, spillover effects related to firm-level capital market responses and corporate policies remain underexplored. Our research provides critical evidence of the spillover effects of market reactions to data breaches among tourism firms and highlights the role of corporate policies in mitigating these effects. This contribution expands the existing literature on spillover effects in the tourism industry.

Finally, we enrich the existing literature by exploring the unique impact of industry-specific characteristics on market reactions to data breaches. Prior research has documented the overall negative impact of data breaches on stock returns (Goel and Shawky, 2009; Malhotra and Malhotra, 2010) and highlighted the moderating roles of firm characteristics (Kannan et al., 2007). However, studies on the spillover effects of data breaches to industry peers present mixed findings, demonstrating both contagion effects (Ettredge & Richardson, 2003; Martin et al., 2017; Kamiya et al., 2021) and competitive spillover effects (Jeong et al., 2019). While general research presents varying outcomes, adverse spillover effects have been particularly evident in the consumer electronics sector, an industry vulnerable to frequent cyberattacks and responsible for managing sensitive customer information (Hinz et al., 2015). Building on these insights, our study investigates the influence of data breaches on both focal firms and their peers in the tourism industry, a sector characterized by unique traits such as high competitiveness (Singal, 2015) and intense service engagement (Koc, 2019). This approach provides a deeper understanding of the sector-specific market responses to data breaches.

2. Background and Hypothesis Development

2.1 Market reactions to data breaches: impact on focal firms

Market reactions to data breaches have been widely studied, with findings indicating that the impact often depends on the nature of the breach and the industry involved. General studies on market reactions to data breaches reveal negative results. Goel and Shawky (2009) examined the impact of security breaches on stock market valuations using an event window spanning 120 days before to 10 days after the breach. Their findings revealed significant negative stock returns concentrated around the event date, underscoring the immediate financial impact of breaches. Similarly, Malhotra and Malhotra (2010) found that customer information breaches led to substantial declines in stock returns, with the severity of the breach amplifying the negative reaction.

Other studies emphasize the role of moderating factors beyond overall effects. For example, the influence of firm characteristics on the degree of market reactions to data breaches. Kannan et al. (2007), who reported insignificant results for their overall sample, attributed this to cross-sectional differences such as firm size and industry. Expanding their research, Yayla and Hu (2011) examine the industry specific market reaction to the data breaches. They found that pure e-commerce firms experienced significantly greater abnormal returns following security breaches compared to traditional brick-and-mortar firms, likely due to their heightened reliance on digital operations. Malhotra and Malhotra (2010) also found that breaches in the financial sector result in negative market reactions due to customer trust issues, whereas Martin et al. (2017) observed less severe reactions in the technology sector, where risks are often considered inherent.

The preceding discussion underscores that certain studies identify a generally significant negative impact of data breaches on focal firms (Goel and Shawky, 2009; Malhotra and Malhotra, 2010). Other research indicates that these negative effects manifest under specific conditions, with characteristics such as sector potentially moderating these impacts (Kannan et al., 2007; Yayla and Hu, 2011; Malhotra and Malhotra, 2010; Martin et al., 2017). However, data breach effects on stock markets are largely uninvestigated in the tourism industry. The tourism sector is highly competitive due to low entry barriers, easy access to labor, and low customer switching costs (Singal, 2015). As such, analyzing market reactions in the tourism industry broadens existing data breach research by emphasizing the role of a sector's competitive dynamics in shaping the effects of data breaches.

2.2 Market reactions to data breaches: impacts on peer firms

The dynamics of contagion and competition following data breaches have drawn significant academic attention. Studies have identified contagion spillover effects, indicating that firms suffer negative market reactions due to the data breaches of their industry peers. For example, Ettredge and Richardson (2003) found that investors reacted negatively to denial-of-service attacks on well-known Internet firms, extending their concerns to "similar" firms due to perceived vulnerabilities, highlighting an interdependence driven by shared reliance on information technology. Similarly, Martin et al. (2017) demonstrated that data breaches generally convey negative information about an entire industry, as evidenced by adverse market reactions affecting peer companies within the same sector. This is further supported by Kamiya et al. (2021), who noted that data breaches result in market value declines for competing firms, affirming their theory on the information content of cyberattacks. Conversely, Jeong et al. (2019) illuminated a competitive spillover effect, showing that some firms gain a competitive advantage following breaches. Their research revealed that approximately ten competitors per breached firm typically experience positive market reactions, suggesting that data breaches can sometimes redistribute market power within industries by highlighting the relative strengths of unaffected firms.

Recent research has sought to clarify the mixed results of data breach spillover effects, uncovering a range of moderating factors. Kashmiri et al. (2017) explored the aftermath of the Target data breach, finding negative abnormal returns for other retailers, with firm size acting as a negative moderator of the contagion effect. They also noted that IT capabilities and corporate social responsibility can mitigate these effects, demonstrating that spillover effects are influenced by firm characteristics. Similarly, Hinz et al. (2015) focused on the consumer electronics industry, finding that data breaches not only led to a decline in share prices for directly affected companies but also for those within the same industry, indicating a contagion effect. The study focused on this industry due to its high frequency of cyberattacks and the sensitivity of the information involved, emphasizing the broader risks posed by data security vulnerabilities within a specific industry.

Research highlights that data breaches typically lead to negative market spillovers (Ettredge and Richardson, 2003; Martin et al., 2017; Kamiya et al., 2021), while also presenting competitive effects (Jeong et al., 2019), resulting in complex and mixed outcomes. However, existing studies examining the moderating factors of data breach spillovers exhibit certain limitations. For instance, some investigations focus exclusively on a single firm (Kashmiri et al., 2017) or prioritize characteristics such as data breach frequency and type, while neglecting other industry-specific factors that may influence spillover effects (Hinz et al., 2015). In contrast, the tourism industry, characterized by its competitiveness (Singal, 2015) and susceptibility to frequent attacks involving sensitive financial information (Chen and Jai, 2019), offers a distinctive context to empirically investigate the peer market reactions to data breaches. This setting allows for an exploration of competitiveness as a potential moderating factor in the diverse outcomes observed across industries.

2.3 Corporate policy changes following data breaches

Another stream of data breach research examines the corporate policies following data breaches. Corporate policy refers to the strategic decisions, guidelines, and practices that a company adopts to achieve its financial and operational objectives (Brealey et al., 2014). Among these policies, cash holdings have received considerable attention due to their critical role in mitigating risks arising from uncertainties (Han and Qiu, 2007; Kusnadi and Wei, 2011;

Chen et al., 2014). One research stream demonstrates the influence of risk on firms' cash holdings decisions. For instance, Duong et al. (2020) find that firms increase cash reserves in response to heightened exposure to policy uncertainty in the U.S. market, using precautionary motives to buffer against financial shocks. Similarly, Lei et al. (2021) show that when a firm's default risk rises, it increases the distress likelihood of related firms, prompting both focal and peer firms to accumulate more cash as a precautionary response to credit risk spillovers. Data breaches introduce significant risk to both focal firms and their industry peers (Schlackl et al., 2021), thus having the possibility to influence the firms' cash holdings. A few research dives into this specific topic. For example, Boasiako and Keefe (2021) demonstrate that firms adjust their cash policies by holding more cash following data breaches, driven by increased regulatory pressure and litigation risks. Further, Garg (2020) emphasizes that data breaches not only impact attacked firms but also have spillover effects on industry peers and related suppliers. Firms in proximity—defined by industry, geography, or supply chain links—tend to increase cash holdings in response to the heightened perceived risk of contagion from breaches.

However, existing studies primarily focus on the general effects of data breaches on cash holdings, overlooking the heterogeneity of industries and specific corporate responses. Notably, the tourism industry presents a unique case for examination. This sector is characterized by significant capital intensity due to substantial investments in real estate and infrastructure, combined with relatively low revenue generation per unit of fixed assets (Singal, 2015). The high requirement for liquidity in tourism firms, coupled with vulnerability to data breaches (Amaro and Duarte, 2015; Law et al., 2014), creates a setting that merits further investigation. Exploring how both focal and peer firms in the tourism industry adjust their corporate cash policies after data breaches will provide deeper insights into risk management strategies in capital-intensive industries.

2.4 Hypothesis development

Data breaches exert a direct and negative influence on the firm value of affected companies. First, data breaches undermine customer satisfaction, which can be analyzed through the framework of gossip theory. Gossip theory posits that when individuals become aware they are the target of gossip, they often respond with negative cognitive and emotional reactions, including feelings of betrayal and violation (Richman and Leary, 2009), hurt and anger (Leary and Leder, 2009), and diminished trust in others (Turner et al., 2003). These reactions occur because individuals are naturally motivated to guard against becoming gossip targets to maintain social standing and group cohesion (Mills, 2010; Baumeister et al., 2004). Data breaches are widely viewed as violations of customer trust, representing a failure by firms to uphold their commitment to safeguarding data privacy (Malhotra and Malhotra, 2011; Rasoulian et al., 2017). Drawing on gossip theory, when a gossip target (customer) perceives vulnerability, such as through the compromise of personal information, their primary responses often manifest as negative cognitive and emotional reactions directed at the gossiper (firm), reflecting the significance of perceived relational threats (Mills, 2010; Richman and Leary, 2009). The tourism sector, characterized by high service involvement (Koc, 2019), is particularly susceptible to such adverse reactions (Migacz et al., 2018; Weber and Sparks, 2009). These reactions can diminish customers' spending behavior (Janakiraman et al., 2018), erode organizational profitability (Hewagama et al., 2019), and negatively influence customer evaluations of service experiences (Ho et al., 2020). Consequently, the market is likely to internalize these customer dissatisfaction outcomes and devalue the affected firm's stock price.

Second, data breaches frequently result in civil and criminal lawsuits, leading to significant financial and reputational damages for firms. Romanosky et al. (2014), drawing on the framework by Cooter and Rubinfeld (1989) that describes how incentives influence decisions regarding litigation initiation, demonstrate that customers are more likely to sue after data breaches when they suffer direct financial harm or when a large number of individuals are affected. The tourism industry, characterized by a high volume of credit card transactions (Chen and Jai, 2019), is particularly vulnerable to breaches involving credit card information, potentially affecting a large number of customers[5] . Consequently, data breaches in the tourism industry may incentivize customers to seek compensation via litigation, which can lead firms to face legal penalties and reputational damage, thus resulting in negative market reactions (Haslem et al., 2017).

In summary, investors devalue the future prospects of breached firms by accounting for the consequences of customer dissatisfaction and associated external risks, which is reflected in declining stock prices once the market absorbs the information about the breach. Based on these insights, this paper proposes the following hypothesis:

H1: Data breaches hurt firm value (in terms of cumulative abnormal stock returns) in the tourism industry.

Data breaches can adversely impact the stock prices of firms operating within the same sector. First, this impact can be explained by the information content theory proposed by Kamiya et al. (2021). The theory suggests that the shareholder lost following data breaches can be demonstrated by adverse updates on key information, including the direct expenses associated with the breach, the likelihood of successful attacks, and the costs required to maintain the attack success rate which investors bear. Data breaches signal to investors that

[5] For example, Marriott disclosed in 2018 through an official statement that information of more than 500 million customers, including names, phone numbers, email addresses and credit card details, had been affected in an identified data breach.

non-disclosing peer firms—for example, those within the same industry or sub-industry—may also be vulnerable to similar crises if data breaches are perceived as systemic, industry-wide issues (Paruchuri and Misangyi, 2015; Lang and Stulz, 1992). This perception heightens concerns about the likelihood of successful attacks, creating a contagion spillover effect that diminishes the stock prices of peer firms within the same sector. Second, in the context of the tourism industry, data breaches heighten investors' concerns about customers' willingness to engage in consumption with peer firms. Roehm and Tybout (2006) argue that scandal spillovers occur across brands when competing brands are strongly associated with the scandalized firm, leading customers to temporarily or permanently shift their preferences away from close competitors. Given that the tourism industry is marked by high levels of competitiveness (Singal, 2015), peer firms within the sector face potential performance decline following data breaches.

Conversely, the adverse information revealed by the attack that is specific to the target can benefit industry competitors, as explained by the information transfer effect. The information transfer effect occurs in the market when newly disclosed information has important implications for the future profitability of other non-announcing competitors, such as intra-industry peers (Jeong et al., 2019). Data breaches may highlight firm-specific weaknesses, highlighting competitors' potential advantages (Jeong et al., 2019; Kamiya et al., 2021). For instance, data breaches can signal deficiencies in a firm's management, undermining previously held perceptions of its capabilities (Kamiya et al., 2021). This, in turn, enhances expectations of competitors' future profitability due to their relative advantage in management quality, particularly in the tourism industry, which is characterized by intense competition (Singal, 2015). As a result, data breaches may lead to a competitive spillover effect within the tourism industry.

Based on these insights, this paper proposes the following hypothesis:

H2: Data breaches have no spillover effects (in terms of cumulative abnormal stock returns) to the sub-industry.

Data breaches compel tourism firms to increase their cash holdings. First, additional capital is required to voluntarily mitigate the impact of service failures caused by data breaches. According to gossip theory, customers react negatively to data breaches in the tourism industry, necessitating firms to allocate resources to service failure recovery to prevent further customer dissatisfaction (Ho et al., 2020) and profitability declines (Hewagama et al., 2019). For instance, firms may need funds to compensate customers affected by data breaches (Rasoulian et al., 2017; Wang et al., 2022a) and to enhance processes to prevent future failures to regain customer trust (Johnston and Michel, 2008; Rasoulian et al., 2017). This demand incentivizes firms to increase cash holdings following data breaches. Second, tourism firms may increase their cash holdings to ensure future debt repayment capability due to the industry's unique characteristic of high leverage ratios. Tourism firms often require substantial capital because of significant investments in real estate and the relatively low revenue generated per unit of fixed assets (Singal, 2015). Additionally, the tourism industry is marked by elevated leverage ratios (Singal, 2015), making it imperative for firms to consistently generate cash to service debt. However, data breaches result in a significant decline in sales growth (Kamiya et al., 2021), restricting firms' income from operating activities. Breached firms also face higher loan spreads, increased collateral requirements, and stricter covenants (Huang and Wang, 2021), limiting their ability to secure additional financing. As a result, tourism firms may increase their cash holdings to maintain investment flexibility and solvency. Third, firms across industries expose themselves to significant litigation risks following data breaches (Romanosky et al., 2014), which ultimately lead to substantial capital expenditures. In summary, tourism firms face heightened demands for cash and limited access to capital, necessitating increased cash holdings in response to data breaches. Based on these insights, this paper proposes the following hypothesis:

H3: Cash holdings increase after firms experience data breaches.

Data breaches have the potential to increase the cash holdings of peer tourism firms within the sub-industry. First, as discussed above, customers of peer firms in the same industry perceive a sense of vulnerability in the form of compromised personal information, as explained by information content theory, leading to negative cognitive and emotional reactions toward the peer firm (Mills, 2010; Richman and Leary, 2009). As a result of these negative reactions, peer firms may experience declines in customer spending and profitability (Janakiraman et al., 2018; Hewagama et al., 2019). The tourism industry, being capital-intensive and highly leveraged (Singal, 2015), as previously discussed, may drive peer firms to increase their cash holdings to compensate for decreased operational income. Second, peer firms may be motivated to engage in data breach prevention measures, thereby requiring greater cash reserves. Negative peer events often lead to information spillovers, conceptually prompting unaffected firms to adopt proactive governance improvements (e.g., Leuz and Wysocki, 2016). Specifically, data breaches encourage peer firms in the same industry to strengthen their internal control systems to reduce the likelihood of future breaches (Ashraf, 2022; Wang et al., 2024). The tourism industry is particularly vulnerable to data breaches in the United States (Amaro and Duarte, 2015; Law et al., 2014). Consequently, we posit that peer firms increase their cash holdings following a data breach to enhance their resilience against potential breaches. Based on these insights, this paper proposes the following hypothesis:

H4: Cash holdings increase after peer firms in the same sub-industry experience data breaches.

3. Methodology

3.1 Data collection and variables

Data for this study were sourced from multiple databases: breach data are collected from the Privacy Rights Clearinghouse (PRC) database, firm financial information is obtained from Compustat, and stock price data are retrieved from the CRSP database. The analysis covers a period from 2005, when the PRC database was initiated, to 2021, which marks the last recorded data breach in the tourism industry within this database. To identify firms affected by data breaches, we merged the Compustat and CRSP databases with the PRC data breach database, aligning the datasets by fiscal year and company name. We also addressed discrepancies in company naming conventions across different databases.[6] Additionally, to minimize the influence of extreme values on estimation results, continuous variables, except for cumulative abnormal returns (CARs), were winsorized at the 99th and 1st percentiles. The final dataset includes 5,883 samples.

[Insert Table 1 about here]

[6] To address the concern that company names in different databases may differ slightly, we identified all firm name pairs between each tourism firm name in firm financial data database and all data breached companies name in PRC which consists at least one same word after dropping the organization type (for example, ltd.) by eliminating the top 100 mostly occurred words in the financial data database and top 20 in data breach database, calculated the pairwise cosine similarity, hand-examined the top three highest cosine similarity of each event date, and retrieve the matched names.

3.2 Cumulative abnormal returns

We employ two models in our main analysis to calculate abnormal returns: the market model (Binder, 1998; MacKinlay, 1997) and the Fama-French three-factor model (Fama and French, 1992). First, we use Equation (1) and Equation (2) to represent the expected stock returns under the market model and the Fama-French three-factor model, respectively:

$$R_{i,t} = \alpha_i + \beta_1 R_{mt} + \varepsilon_{i,t} \quad (1)$$

$$R_{i,t} = R_f + \beta_1 (R_{mt} - R_f) + \beta_2 SMB + \beta_3 HML + \varepsilon_{i,t} \quad (2)$$

where $R_{i,t}$ is expected rate the return of stock i on day t, R_f represents the risk-free return rate, and R_{mt} denotes the return rate of the CRSP value-weighted index. *SMB* (small minus big) captures the return difference between small-cap and large-cap stocks, while *HML* (high minus low) measures the return difference between stocks with high and low book-to-market ratios. The abnormal return for each day is calculated as the difference between the actual return and the expected return, as shown in Equation (3). The expected returns are calculated by Equations (1) and (2), with the parameters estimated over the window [-300, -60] and each data breach event day defined as day 0. Finally, we average the daily abnormal returns within the specified window to obtain the cumulative abnormal return for the window size.

$$AR_{i,t} = R_{i,t} - \widehat{R}_{i,t} \quad (3)$$

3.3 Research models

We employ a fixed-effects regression model to analyze the spillover effects of data breaches.

$$CAR_{i,t} = \alpha_i + \beta_1 SPILLOVER\_HOTEL_{i,t} + \beta_2 SPILLOVER\_REST_{i,t} + \gamma X_{i,t} + Year\ FE + Firm\ FE + \varepsilon_{i,t}, \quad (4)$$

where *i*, *t* represent firms and events, respectively. *CAR* represents cumulative abnormal returns, calculated using market model and Fama-French three-factor model, respectively. *SPILLOVER_HOTEL* and *SPILLOVER_REST* measure spillover effects within the hotel and restaurant sub-industries, respectively. Specifically, *SPILLOVER_HOTEL* (*SPILLOVER_REST*) is assigned a value of one for all firms within the hotel (restaurant) sub-industry if only those firms experience data breaches on the event dates. It is set to zero if no hotel (restaurant) firms experience data breaches or if firms from other sub-industries also report breaches on those dates. For firms in other two sub-industries outside the hotel and restaurant sectors, *SPILLOVER_HOTEL* and *SPILLOVER_REST* are consistently assigned a value of zero. *X* represents control variables, including *ROA*, *Size* and *BM*, consistent with established research on CARs (e.g., Wang et al., 2022b). We also incorporate firm fixed effects (*Firm FE*) and year fixed effects (*Year FE*) to control for unobserved, time-invariant differences across firms. Finally, we apply robust standard error clustering. Our primary focus is on β_1 and β_2, which represent the spillover effects from the hotel and restaurant sub-industries, respectively.

3.4 Descriptive statistics

Table 2 presents the summary statistics of the variables used in our analysis, with the definition of each variable provided in Table 1. The average data breach occurrence rate is 0.012, indicating that approximately 1.2% of observations in the sample experienced data breaches during the study period. The average cash holdings, scaled by sales, for firms in the sample is approximately 55.8% , reflecting a cautious approach to managing financial risk. The observations also show an average book-to-market ratio of 0.437, return-on-assets ratio of 0.007, and leverage ratio of 0.488.

[Insert Table 2 about here]

4. Empirical Results

4.1 Baseline analysis and Robustness tests

Table 3 presents the results of the market reactions for firms reporting data breaches within the tourism industry. A t-test is employed to evaluate the statistical significance of the difference between the abnormal market return and zero. In our baseline analysis, we utilize both the market model and the Fama-French three-factor model to calculate CARs over the seven-day event window [−3,3].

Panel A of Table 3 presents the baseline results examining the market reaction of firms reporting data breaches. The abnormal return is −0.0193 with a t-statistic of −2.03 for the market model, which is significant at the 5% level (column 1). Similarly, the Fama-French three-factor model shows an abnormal return of −0.0171 and a t-statistic of −1.84, also significant at the 5% level (column 2). These findings support H_1, which indicates that the market reacts negatively to data breaches in the tourism industry.

Further robustness tests are reported in Panel B, where we employ alternative models and varying window sizes. First, we evaluate CARs over the seven-day event window using the Fama-French four-factor model, which yields an abnormal return of −0.0227 and a t-statistic of −2.43, statistically significant at the 5% level. This result underscores the negative market response to data breaches in the tourism industry and demonstrates that the baseline analysis is robust to different models. Additionally, we assess CARs over a five-day window surrounding the event day, using both the market model and the Fama-French three-factor model, consistent with the baseline analysis. For the market model, the abnormal return is −0.0129 with a t-statistic of −1.77 (column 1), while the Fama-French three-factor model reports an abnormal return of −0.0128 with a t-statistic of −1.82 (column 2), both of which are statistically significant at the 5% level. These findings confirm that the market reacts negatively to data breaches in the tourism industry and that the baseline analysis is robust to variations in event windows. In summary, the results demonstrate that the main findings are consistent across different models and event windows, confirming the robustness of the main regression results.

Overall, the findings from both panels confirm a consistent negative market reaction to data breaches in the tourism industry, with the degree of significance varying by model and time window. The robustness of these results across different methodologies highlights a reliable negative association between data breaches and market performance.

4.2 Market reactions to data breaches across sub-industries

In this section, we investigate the effects of data breaches on firm value across various sectors within the tourism industry. Utilizing the GIC sub-industries (GSUBIND) to identify tourism sub-industries (Gao and Zhang, 2023), we classify data breaches into four primary sectors: airline, hotel, restaurant, and casino. The dataset comprises 5, 31, 22, and 7 reported data breaches for the airline, hotel, restaurant, and casino sub-industries, respectively. Given that three of the four sub-industries exhibit a small sample size ($N < 30$), we apply a bootstrapping technique to expand each sub-industry sample to 50 observations before conducting our analyses. Panel C reveals that both the hotel sector (CAR of -0.0360, t = -2.43 for the market model; CAR of -0.0325, t = -2.35 for the Fama-French three-factor model) and the restaurant sector (CAR of -0.0254, t = -1.76 for the market model; CAR of -0.0228, t = -1.87 for the Fama-French three-factor model) exhibit significant negative cumulative abnormal returns following data breaches. In contrast, the airline and casino sectors do not consistently show significant results. These findings indicate that the negative market reactions to data breaches in the tourism industry are primarily driven by the hotel and restaurant sub-industries.

[Insert Table 3 about here]

5. Spillover effect of market reactions

5.1 Sub-industry data breach spillover effects

In this section, we test the hypothesis that peer firms also experience negative market reactions following data breaches. Building on the results from Section 4.2, which indicated that negative market reactions are primarily observed in the hotel and restaurant sectors, we examine whether data breaches in these sectors, which negatively impact focal firms, also influence their sub-industry peers. To test this hypothesis, we employ Equation (4), using two indicator variables—*SPILLOVER_HOTEL* and *SPILLOVER_REST*—to measure spillover effects in the hotel and restaurant sub-industries, respectively.

[Insert Table 4 about here]

The results presented in Table 4 demonstrate that both the hotel and restaurant sub-industries experience significant negative spillover effects following data breaches. Specifically, when data breaches occur within the hotel sub-industry, the cumulative abnormal returns decrease by -0.0154 or -0.0112, depending on the model employed, compared to the abnormal returns of other firm-event days in the sample. These results are significantly negative at the 1% level, indicating that peer firms in the hotel sub-industry experience substantial negative abnormal returns. Similarly, the restaurant sub-industry exhibits negative abnormal returns, with a 1% level significant difference of -0.0201 in the market model and a 5% level significant difference of -0.0224 in the Fama-French three-factor model during event dates, compared to the abnormal returns of other firm-event days in the sample. These findings suggest that peer firms in the restaurant sub-industry also experience significantly negative abnormal returns. Collectively, these regression results support H_2 that data breaches create contagion spillover effects.

5.2 Heterogeneity tests

In this section, we examine the impact of various moderators on the spillover effects in the hotel and restaurant sub-industries. *Moderator* includes *Customer*, *Size*, *Disclose*, and *Repeat*. Our interest is to identify β_3 and β_4, which represent the moderating influence of different variables on the spillover effect in two sub-industries, respectively.

$$CAR_{i,t} = \alpha_i + \beta_1\, SPILLOVER\_HOTEL_{i,t} + \beta_2\, SPILLOVER\_REST_{i,t} + \beta_3 SPILLOVER\_HOTEL_{i,t} * Moderator + \beta_4\, SPILLOVER\_REST_{i,t} * \text{Moderator} + \gamma X_{i,t} + Year\ FE + \varepsilon_{i,t}, \quad (5)$$

where *Moderator* is one of the four previously mentioned indicator variables. The PRC database provides descriptions of each data breach, enabling us to identify instances involving customer information leakage (*Customer*). This information encompasses individual names, addresses, credit card numbers, Social Security numbers, email addresses, and phone numbers. Furthermore, we note from the PRC database that some firms disclose the number of records affected by the breach while others do not. To capture this distinction, we construct an indicator variable, *Disclose*, which represents the differing response strategies regarding the disclosure of affected records. In terms of firm characteristics, we incorporate the size (*Size*) of the data breach firms as a characteristic in our analysis. Finally, we categorize the data breaches within each sub-industry chronologically, using the variable *Repeat* to denote instances of second or subsequent data breaches occurring within the same sub-industry during a fiscal year. Other variables are consistent with Equation (4).

5.2.1 Data breach type

The nature of the data compromised influences the extend of the spillover effect of data breach on stock return. Data breaches fundamentally represent a violation of customer trust, undermining the assurance that personal data is securely protected (Malhotra and Malhotra, 2011). Data breaches involving the leakage of sensitive customer information, such as individual names, addresses, credit card numbers, Social Security numbers, email addresses, and phone numbers, are likely to generate a heightened sense of violation. Consequently, these incidents may result in significantly larger negative abnormal returns compared to breaches of less sensitive information. Supporting this assertion, Kamiya et al. (2021) found that firms experiencing attacks resulting in the loss of personal financial information faced substantial shareholder wealth losses. Building on our earlier findings in Section 5.1, which highlighted the spillover effects of data breaches on stock returns, we further investigate the moderating impact of customer information leakage on these spillover effects.

To examine this hypothesis, we categorize firms based on whether their data breaches involved the access of sensitive customer information. *Customer* is an indicator variable that equals one if data breaches result in customer information leakage. Following this classification, we examine the moderating impact of data breach types on the spillover effects through Equation (5). The results, presented in Panel A of Table 5, reveal that the interaction coefficient of *SPILLOVER_HOTEL* and *Customer* is -0.0264 in column (1) and -0.0240 in column (2), statistically significant at the 1% and 5% levels, respectively. This finding indicates that data breaches involving customer information yield a more pronounced contagion spillover effect on market reactions, consistent with our initial expectations.

5.2.2 Transparency

Customer trust violations resulting from data breaches can be alleviated through transparency, particularly by disclosing detailed information about the breach (Martin et al. 2017). To test this hypothesis, we conducted a regression analysis using using the disclosure of the number of records affected by the breach, as recorded in the PRC database, as a proxy for data breach transparency. *Disclose* is an indicator variable that equals one if data breach firms disclose the number of data affected.

The results are presented in Panel B of Table 5. The interaction term of *SPILLOVER_REST* and *Disclose* is significant at 1% level in both models, with coefficients of 0.0450 and 0.0439, respectively. The positive and significant interaction indicates that when restaurant firms experience spillover effects and disclose the number of customers affected, there is a corresponding positive impact on stock returns. These findings suggest that disclosure practices within the restaurant industry help mitigate the negative spillover effects associated with data breaches, aligning with our predictions.

5.2.3 Firm size

In this section, we examine the potential moderating effects of firm size on spillover effects. The existing literature in the finance industry establishes a negative relationship between firm size and average returns (Fama and French, 1995; Banz, 1981), primarily because smaller firms are often associated with higher distress risks. In contrast, larger firms typically possess more resources—such as capital, personnel, and backup services—enabling them to mitigate the impact on stock returns more effectively than their smaller counterparts (Kannan et al., 2007). Based on this, we hypothesize that the spillover effect will differ between large and small firms, with larger breach firms exhibiting a reduced spillover effect on the sector.

To test this hypothesis, we partition the firms based on whether their size exceeds the median size of all breach firms within their respective sub-industry for the relevant fiscal year. We then conduct regression analysis. The results are presented in Panel C of table 5. The coefficient of interaction of *SPILLOVER_REST* and *SizeD* is 0.0375 in column (1) and 0.0379 in column (2), both of which are significantly negative at 1% level. This finding suggests that larger firm size mitigates the contagion spillover effect on market reactions, aligning with our initial expectations.

Additionally, we conducted untabulated tests to explore the moderating effect of peer firms' size. These analyses did not yield significant results, indicating that the spillover effect is unaffected by the size of peer firms within the sub-industry.

5.2.4 Repeated data breach

The recurrence of data breaches can significantly amplify the negative market reactions. When a firm experiences multiple data breaches in a relatively short timeframe, the damage to customer trust can be exacerbated, resulting in a more substantial decline in firm value during the second or subsequent breaches. Peng et al. (2023) indicated that firm value of the first two data breaches within a year differs, with the second breach having a notably greater negative impact than the first.

In light of this finding, we hypothesize that the frequency of data breaches within fiscal years is likely to contribute to the extent of spillover effects. The results, presented in Panel D of Table 5, show that the interaction coefficient for *SPILLOVER_HOTEL* and *Repeat* is -0.0295 in column (1) and -0.0289 in column (2), both statistically significant at the 5% level. These findings underscore that repeated data breaches amplify the contagion spillover effect on market reactions, aligning with the conclusions of Peng et al. (2023).

[Insert Table 5 about here]

6. Corporate policy following data breaches

In this section, we explore the implications of data breaches on corporate policy. We adapt the following equation to investigate the effect of corporate policy on data breaches.

$$Corporate\ policy_{i,t} = \alpha_i + \beta_1\ DATABREACH_{i,t\text{-}1} + \gamma X_{i,t\text{-}1} + Year\ FE + Firm\ FE + \varepsilon_{i,t\text{-}1}, \quad (7)$$

Where corporate policy is either cash holdings or dividend per share. We define cash holdings as cash plus marketable securities divided by sales, following Hanlon et al. (2017). We define dividend per share as the cash dividend paid scaled by the common shares following Hossain et al. (2023) and Tao et al. (2022). $DATABREACH_{i,t\text{-}1}$ is an indicator that equals to one if firm *i* experienced a data breach at year *t-1*. $X_{i,t\text{-}1}$ represents control variables, which are defined below.

6.1 Cash holdings following data breaches

Panel A of table 6 presents the result of testing H_3 using the regression specified in Equation (7). Column (1) in Panel A of Table 6 includes all observations of firms that experienced data breaches in our sample period. Column (2) and (3) further disaggregate the sample into sub-industries.

Following Hanlon et al. (2017) and Lee and Powell (2011), we include *BM*, *LEV*, *Size*, *Net Working Capital*, *CFO*, *CFOVAR*, *INVEST*, *Z_SCORE* as control variables. *BM* is expected to have a positive relationship with cash holdings, as firms with better growth opportunities tend to retain more cash for funding growth. Conversely, *INVEST* is negatively correlated with cash holdings, suggesting that higher levels of investment decrease available cash. *CFO* and *CFOVAR* also have a positive relationship with cash holdings, as firms with robust operating cash flows and lower cash flow variance typically retain more cash. Previous research indicated that firms with better access to capital usually maintain lower cash balances (Mulligan, 1997), suggesting a negative correlation between *Size*, *Net Working Capital*, and *Z-Score* with cash holdings. Additionally, LEV has been shown to exhibit both positive and negative relationships with cash holdings (Hanlon et al., 2017).

We begin by regressing on the entire data breach sample, which includes all firms that reported data breaches from 2005 to 2021. The coefficient of *DATABREACH* in column (1) in Panel A of Table 6 is 0.0684, statistically significant at 5% level. This indicates that data breaches are associated with a 7% increase in cash holdings relative to sales in the following year. This result supports H3, showing that cash holdings are significantly higher in the year following data breach events compared to other years. The coefficient of *DATABREACH* in column (2) and column (3) is 0.1597 and -0.0148, with the former being statistically significant at 1% level and the latter statistically insignificant. This suggests that the observed effect in column (1) is largely driven by the hotel sub-industry.

Next, we examine the spillover effects of data breaches on cash holdings in firms within the same sub-industry that did not experience breaches themselves, as detailed in Panel B of Table 6. The coefficient of *Spill* is 0.0267 and is statistically significant at the 5% level, indicating that firms increase their cash holdings in the year following data breaches by sub-industry peers. When disaggregating data breaches by sub-industry, the coefficient of *Spill* is 0.1054 in the hotel sub-industry and 0.0178 in the other three sub-industries, statistically significant at the 10% and 1% levels, respectively. These findings suggest that firms increase their cash holdings in response to data breaches involving peer firms within the same sector, supporting our hypothesis that cash holdings increase following data breaches experienced by sub-industry peers.

Finally, we investigate the spillover effects of data breaches on cash holdings across different sub-industries, as detailed in Panel C. Specifically, we analyze how breaches in one sub-industry influence cash holdings in firms from the remaining three sub-industries. In column (1), *SPILL_OTHERS* equals 1 if the hotel sub-industry experienced a data breach during the previous year, with the sample including all firms from the restaurant, airline, and casino sub-industries from 2005 to 2021, excluding those that experienced data breaches. In columns (2) to (4), the variable *SPILL_OTHERS* equals 1 if the restaurant, casino, and airline sub-industries, respectively, experienced data breaches during the previous year. The sample consistently excludes observations that reported breaches during the same period. The coefficient of *SPILL_OTHERS* in column (1) is 0.0256, statistically significant at the 1% level. In contrast, the coefficients in columns (2) to (4) are not statistically significant. These results indicate that firms in other sub-industries increase their cash holdings following data breaches in the hotel sub-industry.

[Insert Table 6 about here]

6.2 Dividend payouts following data breaches

We also examine changes in dividend payouts by focal and peer firms following data breaches. Customers' sense of vulnerability due to data breaches, as described by gossip theory, diminishes their spending behavior (Janakiraman et al., 2018) and erodes organizational profitability (Hewagama et al., 2019). Research demonstrated that the perceived stability of future earnings is a key factor influencing dividend policy (Lintner, 1956; Brav et al., 2005). Therefore, we hypothesize that focal firms reduce dividend payouts following data breaches. Peer firms may also decrease their dividend payouts for similar reasons. However, as dividend payouts are widely recognized as an effective corporate policy to address the free cash flow problem (e.g., La Porta et al., 2000; Chen et al., 2017), peer firms might choose to maintain their dividend payouts following data breaches in their sub-industry to mitigate potential agency problems.

Following Ni et al. (2020) and Hossain et al. (2023), we include *Size*, *ROA*, *CASH*, *BM*, *LEV*, *Tangibility*, *Volatility*, *Age* as control variables. Larger firms are more likely to distribute dividends due to reduced financial constraints (Hail et al., 2014); therefore, we control for firm size in our analysis. A lack of investment opportunities, as proxied by *BM*, is positively related to dividend payouts. We include *ROA* and *Volatility* to control the influence of firm performance on dividend payouts. Specifically, *ROA* demonstrates a positive relationship with dividend payouts, whereas *Volatility* is negatively associated with dividend payouts. Furthermore, previous research identified both positive and negative effects of cash and asset tangibility on dividend payouts (Hasan and Uddin, 2022; Koo et al., 2017). We also incorporate firm age to control for the positive effect of accumulated resources on dividend payouts and *LEV* to control for borrowing costs.

We commence our analysis with the data breach sample that includes all firms that reported data breaches from 2005 to 2021. Panel A of table 6 presents the result using the regression specified in Equation (7). Column (1) includes all observations of firms that experienced data breaches in our sample period. Column (2) and (3) further disaggregate the sample into sub-industries. The coefficient of *DATABREACH* in column (1) in Panel A of Table 7 is -0.1556, which is statistically significant at 5% level. This finding indicates that data breaches lead to a 16% decrease in dividends per share in the year following the breach. The coefficients of *DATABREACH* in column (2) and column (3) is -0.2578 and -0.0273, respectively, with the former being statistically significant at the 5% level. This result further shows that the effect is primarily driven by the hotel sub-industry.

We further investigate the spillover effect of data breaches on the dividend per share of firms within the same sub-industry as those that experienced breaches, as shown in panel B of table 7. Observation that reported breaches in the same period are excluded from the analysis.

The coefficient of *Spill* is 0.0197 in column (1), 0.0075 in column (2), and 0.0239 in column (3) , none of which are statistically significant. These results indicate that firms do not adjust their payout policy in response to data breaches among peer firms in the same sub-industry. A possible explanation is that peer firms leverage dividend payouts to address agency problems, as suggested by the agency theory (La Porta et al, 2000; Chen et al., 2017), as discussed earlier.

Next, we explore the spillover effect of data breaches on dividend payouts across sub-industries in panel C. Specifically, we look at the influence of data breach events on dividend per share of peer firms in the other three sub-industries. In column (1), *SPILL_OTHERS* equals to 1 if hotel sub-industry experienced data breach during the following year and the sample includes all firms in restaurant, airline, and casino sub-industries from 2005 to 2021, excluding those that experienced data breaches. In columns (2) to (4), the variable *SPILL_OTHERS* equals to 1 if the restaurant, casino, and airline sub-industries, respectively, experienced data breaches. The sample consistently excludes all observations that report data breaches during the same period. Similarly to panel B, the coefficients of column (1) to (4) are not significant. The combined results of Panel B and Panel C indicate that firms do not alter their payout policies in response to the decrease in dividend payouts experienced by peer firms due to data breaches.

[Insert Table 7 about here]

7. Conclusion

With the proliferation of digital information, data breaches have become more frequent and increasingly costly for firms. Although a growing body of literature explores data breaches, there remains a significant gap in research examining their consequences and spillover effects within the tourism industry.

This paper examines the impact of data breaches from the perspectives of investors and managers. The findings demonstrate that data breaches have a significant negative effect on cumulative abnormal returns, a result that remains robust across various models and event window sizes. This negative impact is primarily concentrated in the restaurant and hotel sub-industries, where significant contagion effects are also observed. The analysis further explores the corporate policies adopted in response to data breaches. The results indicate that data breaches prompt firms to increase cash holdings while reducing dividend payouts, with these effects being exclusive to the hotel sub-industry. Additionally, the examination of spillover effects reveals significant contagion effects on cash holdings among peer firms, although no similar impact on dividend payouts is observed.

Our findings provide a novel perspective on the impact of data breaches in the tourism industry, highlighting their effects on market reactions and corporate policy adjustments. Furthermore, we offer unique evidence on how a firm's response to data breaches affects its industry peers, considering the perspectives of both investors and managers. Additionally, our work contributes to the literature by examining the specific effects of industry characteristics on market reactions to data breaches, focusing on differences in consequences and risk management strategies within the tourism industry, and expanding upon how firms adjust their cash holdings in response to these events.

Our research has several limitations. First, after merging the databases, the resulting dataset is relatively small in size. Second, the method used to define sub-industries does not fully isolate the tourism industry. For instance, local residents dining at neighborhood restaurants are included in our analysis, even though such customer actions do not strictly fall under tourism. However, due to the limitations of available data, we are currently unable to address these issues comprehensively.

References

Amaro, S., & Duarte, P. (2015). An integrative model of consumers' intentions to purchase travel online. Tourism management, 46, 64-79.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. The Accounting Review, 97(2), 1-24.

Banz, R. W. (1981). The relationship between return and market value of common stocks. Journal of financial economics, 9(1), 3-18.

Baumeister, R. F., Zhang, L., & Vohs, K. D. (2004). Gossip as cultural learning. Review of general psychology, 8(2), 111-121.

Binder, J. (1998). The event study methodology since 1969. Review of quantitative Finance and Accounting, 11, 111-137.

Boasiako, K. A., & Keefe, M. O. C. (2021). Data breaches and corporate liquidity management. European Financial Management, 27(3), 528-551.

Boto-García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. Journal of Hospitality and Tourism Management, 55, 240-247.

Bovsh, L., Bosovska, M., Okhrimenko, A., & Rasulova, A. (2023). Digital security of the hotel brand. Менаџмент у хотелијерству и туризму, 11(1), 145-163.

Brav, A., Graham, J. R., Harvey, C. R., & Michaely, R. (2005). Payout policy in the 21st century. Journal of financial economics, 77(3), 483-527.

Brealey, R. A., Myers, S. C., & Allen, F. (2014). Principles of corporate finance. McGraw-hill.

Chen, H. S., & Jai, T. M. C. (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. International Journal of Hospitality Management, 82, 326-334.

Chen, D., Li, S., Xiao, J. Z., & Zou, H. (2014). The effect of government quality on corporate cash holdings. Journal of Corporate Finance, 27, 384-400.

Chen, J., Leung, W. S., & Goergen, M. (2017). The impact of board gender composition on dividend payouts. Journal of Corporate finance, 43, 86-105.

Chen, R. R., Guedhami, O., Yang, Y., & Zaynutdinova, G. R. (2020). Corporate governance and cash holdings: Evidence from worldwide board reforms. Journal of Corporate Finance, 65, 101771.

Cooter, R. D., & Rubinfeld, D. L. (1989). Economic analysis of legal disputes and their resolution. Journal of economic literature, 27(3), 1067-1097.

Duong, H. N., Nguyen, J. H., Nguyen, M., & Rhee, S. G. (2020). Navigating through economic policy uncertainty: The role of corporate cash holdings. Journal of Corporate Finance, 62, 101607.

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

Fama, E. F., & French, K. R. (1992). The cross‐section of expected stock returns. the Journal of Finance, 47(2), 427-465.

Fama, E. F., & French, K. R. (1995). Size and book‐to‐market factors in earnings and returns. The journal of finance, 50(1), 131-155.

Gao, J., & Zhang, L. (2024). Climate policy uncertainty and corporate investment: Evidence from the US tourism and hospitality sector. Journal of Travel Research, 63(2), 517-530.

Gao, Y. L., Zhang, L., & Wei, W. (2021). The effect of perceived error stability, brand perception, and relationship norms on consumer reaction to data breaches. International Journal of Hospitality Management, 94, 102802.

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. Financial Management, 49(2), 503-519.

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

Hail, L., Tahoun, A., & Wang, C. (2014). Dividend payouts and information shocks. Journal of Accounting Research, 52(2), 403-456.

Han, S., & Qiu, J. (2007). Corporate precautionary cash holdings. Journal of corporate finance, 13(1), 43-57.

Hanlon, M., Maydew, E. L., & Saavedra, D. (2017). The taxman cometh: Does tax uncertainty affect corporate cash holdings?. Review of Accounting Studies, 22, 1198-1228.

Hasan, M. M., & Uddin, M. R. (2022). Do intangibles matter for corporate policies? Evidence from organization capital and corporate payout choices. Journal of Banking & Finance, 135, 106395.

Haslem, B., Hutton, I., & Smith, A. H. (2017). How much do corporate defendants really lose? A new verdict on the reputation loss induced by corporate litigation. Financial Management, 46(2), 323-358.

Hewagama, G., Boxall, P., Cheung, G., & Hutchison, A. (2019). Service recovery through empowerment? HRM, employee performance and job satisfaction in hotels. International journal of hospitality management, 81, 73-82.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. Information & Management, 52(3), 337-347.

Ho, T. H., Tojib, D., & Tsarenko, Y. (2020). Human staff vs. service robot vs. fellow customer: Does it matter who helps your customer following a service failure incident?. International Journal of Hospitality Management, 87, 102501.

Hossain, M. N., Rabarison, M. K., Ater, B., & Sobngwi, C. K. (2023). CEO marital status and dividend policy. Journal of Corporate Finance, 78, 102342.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. The Accounting Review, 96(3), 261-286.

IBM. (2023). “Cost of a Data Breach Report 2023,” Retrieved from https://www.ibm.com/reports/data-breach

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.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), 681-695.

Johnston, R., & Michel, S. (2008). Three outcomes of service recovery: Customer recovery, process recovery and employee recovery. International Journal of Operations & Production Management, 28(1), 79-99.
Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749.
Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12(1), 69-91.
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, 208-228.
Koc, E. (2019). Service failures and recovery in hospitality and tourism: A review of literature and recommendations for future research. Journal of Hospitality Marketing & Management, 28(5), 513-537.
Koo, D. S., Ramalingegowda, S., & Yu, Y. (2017). The effect of financial reporting quality on corporate dividend policy. Review of Accounting studies, 22, 753-790.
Kusnadi, Y., & Wei, K. J. (2011). The determinants of corporate cash management policies: Evidence from around the world. Journal of Corporate Finance, 17(3), 725-740.
La Porta, R., Lopez ‐ de ‐ Silanes, F., Shleifer, A., & Vishny, R. W. (2000). Agency problems and dividend policies around the world. The journal of finance, 55(1), 1-33.
Lang, L. H., & Stulz, R. (1992). Contagion and competitive intra-industry effects of bankruptcy announcements: An empirical analysis. Journal of financial economics, 32(1), 45-60.
Law, R., Buhalis, D., & Cobanoglu, C. (2014). Progress on information and communication technologies in hospitality and tourism. International journal of contemporary hospitality management, 26(5), 727-750.
Leary, M. R., & Leder, S. (2009). The nature of hurt feelings: Emotional experience and cognitive appraisals. Feeling hurt in close relationships, 15-33.
Lee, E., & Powell, R. (2011). Excess cash holdings and shareholder value. Accounting & Finance, 51(2), 549-574.
Lei, J., Qiu, J., Wan, C., & Yu, F. (2021). Credit risk spillovers and cash holdings. Journal of Corporate Finance, 68, 101965.
Leuz, C., & Wysocki, P. D. (2016). The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. Journal of accounting research, 54(2), 525-622.
Lintner, J. (1956). Distribution of incomes of corporations among dividends, retained earnings, and taxes. The American economic review, 46(2), 97-113.
MacKinlay, A. C. (1997). Event studies in economics and finance. Journal of economic literature, 35(1), 13-39.
Ma, T., Hong, T., & Zhang, H. (2015). Tourism spatial spillover effects and urban economic growth. Journal of Business Research, 68(1), 74-80.
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.

Mao, Z. E., & Yang, Y. (2016). FDI spillovers in the Chinese hotel industry: The role of geographic regions, star-rating classifications, ownership types, and foreign capital origins. Tourism Management, 54, 1-12.

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

Migacz, S. J., Zou, S., & Petrick, J. F. (2018). The "terminal" effects of service failure on airlines: Examining service recovery with justice theory. Journal of Travel Research, 57(1), 83-98.

Mills, C. (2010). Experiencing gossip: The foundations for a theory of embedded organizational gossip. Group & Organization Management, 35(2), 213-240.

Mitra, S. K., Chattopadhyay, M., & Jana, R. K. (2019). Spillover analysis of tourist movements within Europe. Annals of tourism research, 79, 102754.

Mulligan, C. B. (1997). Scale economies, the value of time, and the demand for money: Longitudinal evidence from firms. Journal of Political Economy, 105(5), 1061-1079.

Ni, X., Song, W., & Yao, J. (2020). Stakeholder orientation and corporate payout policy: Insights from state legal shocks. Journal of Banking & Finance, 121, 105970.

Park, J., Shin, W., Kim, B., & Kim, M. (2024). Spillover effects of data breach on consumer perceptions: evidence from the E-commerce industry. Internet Research.

Paruchuri, S., & Misangyi, V. F. (2015). Investor perceptions of financial misconduct: The heterogeneous contamination of bystander firms. Academy of Management Journal, 58(1), 169-194.

Peng, J., Zhang, H., Mao, J., & Xu, S. (2023). Repeated data breaches and firm value. Economics Letters, 224, 111001.

PricewaterhouseCoopers (PwC). (2023). PwC's 26th Annual Global CEO Survey (Winning today's race while running tomorrow's), Retrieved from https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey-2023.html

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2017). Service crisis recovery and firm performance: Insights from information breach announcements. Journal of the Academy of Marketing Science, 45, 789-806.

Roehm, M. L., & Tybout, A. M. (2006). When will a brand scandal spill over, and how should competitors respond?. Journal of Marketing Research, 43(3), 366-373.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. Journal of Empirical Legal Studies, 11(1), 74-104.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. Information & Management, 59(4), 103638.

Singal, M. (2015). How is the hospitality and tourism industry different? An empirical test of some structural characteristics. International Journal of Hospitality Management, 47, 116-119.

Smart Richman, L., & Leary, M. R. (2009). Reactions to discrimination, stigmatization, ostracism, and other forms of interpersonal rejection: a multimotive model. Psychological review, 116(2), 365.

Statistisa. (2023). “Average cost of a data breach in the United States from 2006 to 2023”, Retrieved from https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

Tao, Q., Wei, K. J., Xiang, X., & Yi, B. (2022). Board directors' foreign experience and firm dividend payouts. Journal of Corporate Finance, 75, 102237.

Turner, M. M., Mazur, M. A., Wendel, N., & Winslow, R. (2003). Relational ruin or social glue? The joint effect of relationship type and gossip valence on liking, trust, and expertise. Communication Monographs, 70(2), 129-141.

Wang, T., Yen, J. C., & Yoon, K. (2022b). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. International Journal of Accounting Information Systems, 46, 100567.

Wang, J., Wu, Z., Yuan, X., & Song, Z. (2024). Peer governance effects of information security breaches. Energy Economics, 129, 107264.

Wang, X., Wang, X., Liu, Z., Chang, W., Hou, Y., & Zhao, Z. (2022a). Too generous to be fair? Experiments on the interplay of what, when, and how in data breach recovery of the hotel industry. Tourism Management, 88, 104420.

Weber, K., & Sparks, B. (2009). The effect of preconsumption mood and service recovery measures on customer evaluations and behavior in a strategic alliance setting. Journal of Hospitality & Tourism Research, 33(1), 106-125.

Xu, Y., Chen, X., Nicolau, J. L., & Luo, P. (2023). Trust transfer in peer-to-peer accommodation: Does booking with one host transfer to other listings by the same host?. Annals of Tourism Research, 101, 103603.

Xu, Y., Nicolau, J. L., & Luo, P. (2022). Travelers’ reactions toward recommendations from neighboring rooms: Spillover effect on room bookings. Tourism Management, 88, 104427.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. Journal of Information Technology, 26(1), 60-77.

Table 1 Variable Definitions

Variable	Description
Dependent variables	
CARs (*CAR*)	Cumulative Abnormal Returns, calculated by market model and Fama–French three-factor model over window [-3,3] in baseline analysis, and calculated by Fama–French four-factor model over window [-3,3] and by market model and Fama–French three-factor model over window [-2,2] in robustness tests.
Cash holdings *(CASH)*	Cash plus marketable securities divided by sales.
Dividend payouts *(DPS)*	Total cash dividends divided by common shares outstanding.
Independent variables	
DATABREACH	Indicator variable that equals one for firms that have data breaches at event dates, and zero otherwise.
SPILL	Indicator variable that equals one for all sub-industry firms if firms from the same sub-industry have data breaches at event dates, and zero otherwise.
SPILLOVER_HOTEL	Indicator variable that equals one for all hotel sub-industry firms if only hotel sub-industry firms have data breaches at event dates, and zero otherwise.
SPILLOVER_REST	Indicator variable that equals one for all restaurant sub-industry firms if only restaurant sub-industry firms have data breaches at event dates, and zero otherwise.
SPILL_OTHERS	Indicator variable that equals one for all sub-industry firms if only firms from other sub-industries have data breaches at event dates, and zero otherwise.
Control variables	
Age	Firm age, defined as the natural log of the difference between current year and the first year in Compustat plus one.
BM	Book-to-market ratio, defined as total common Equity divided by market value.
CFO	Operating cash flow divided by total assets.
CFOVAR	Standard deviation of the first difference of operating cash flow of last three years.
Customer	Indicator variable that equals one if data breaches result in customer information leakage, and zero otherwise.
Disclose	Indicator variable that equals one if data breach firms disclose the number of data affected, and zero otherwise.
INVEST	Investment, defined as the ratio of capital expenditures to total assets.
LEV	Leverage, defined as long-term debt plus debt in current liabilities, divided by total assets.
Net working capital	Net working capital, defined as the difference between working capital and cash holdings scaled by total assets.
Repeat	Indicator variable that equals one if the data breach is the second or more in the sub-industry in a fiscal year, and equals zero if is the first in the year with at least two data breaches.
ROA	Return on assets, defined as the net profits divided by total assets.
Size	Firm size, defined as the natural log of total assets.
SizeD	Indicator variable that equals one if the size of data breach firms is larger than the median size of all sub-industry breach firms in event fiscal year, and zero otherwise.
Tangibility	Ratio of net property, plant, and equipment to total assets.
Volatility	Standard deviation of the monthly stock return of the year.

Z_SCORE	Altman's Z-score, defined as $1.2 \times X_1 + 1.4 \times X_2 + 3.3 \times X_3 + 0.6 \times X_4 + 0.999 \times X_5$, where X_1 is working capital scaled by total assets, X_2 is retained earnings scaled by total assets, X_3 is earnings before interest and tax scaled by total assets, X_4 is market value of equity scaled by total assets, and X_5 is net sales scaled by total assets.

Table 2 Summary statistics

This table presents the summary statistics of variables used in the analysis. All variables are defined in Table 1. All continuous variables, apart from CARs, are winsorized at the 1% level at both tails of their distributions. We show summary statistics of all tourism industry companies at all event dates and summary statistics of data breach companies at their event dates. ***, **, and * indicate the subsamples are significantly different from each other at the 1%, 5%, and 10% levels, respectively.

	Full sample N=5826				
	Mean	Median	STD	Q1	Q3
	(1)	(2)	(3)	(4)	(5)
Market [-2, 2]	-0.006	-0.004	0.079	-0.033	0.024
Fama-French 3 Factor [-2,2]	-0.005	-0.003	0.077	-0.033	0.024
Market [-3,3]	-0.008	-0.004	0.093	-0.04	0.028
Fama-French 3 Factor [-3,3]	-0.006	-0.004	0.091	-0.038	0.028
Fama-French 4 Factor [-3,3]	-0.007	-0.004	0.091	-0.039	0.027
CASH	0.558	0.133	11.289	0.046	0.292
DPS	1.225	0.082	3.009	0.000	0.986
DATABREACH	0.012	0.000	0.107	0.000	0.000
SPILL	0.915	1.000	0.279	1.000	1.000
SPILL_OTHERS	0.761	1.000	0.427	1.000	1.000
Age	2.830	2.890	0.762	2.303	3.367
BM	0.437	0.314	0.643	0.124	0.622
CFO	0.082	0.087	0.105	0.046	0.132
CFOVAR	0.006	0.001	0.018	0.000	0.004
Customer	0.100	0.000	0.300	0.000	0.000
Disclose	0.196	0.000	0.397	0.000	0.000
INVEST	0.062	0.048	0.054	0.020	0.086
LEV	0.488	0.466	0.399	0.250	0.650
Net working capital	-0.118	-0.103	0.098	-0.168	-0.057
Q	2.079	1.523	1.691	1.185	2.232
Repeat	0.248	0.000	0.432	0.000	0.000
ROA	0.007	0.028	0.137	-0.017	0.066
Size	7.302	7.305	1.996	5.837	8.864
SizeD	0.174	0.000	0.379	0.000	0.000
Tangibility	0.486	0.557	0.276	0.217	0.715
Volatility	0.121	0.106	0.063	0.076	0.148
Z_SCORE	0.074	0.168	0.800	-0.052	0.444

Table 3 Data Breach and Cumulative Abnormal Return: t-test

This table presents the t-test result of CARs in the data breach sample. Panel A reports the baseline analysis result of CARs calculated by market model and Fama–French three-factor model over a seven-day window [-3,3]. Pabel B reports robustness tests results using the alternative Fama-French 4 factor model and the five-day window [-2, 2], respectively. Panel C presents t-test results of data breach sample CARs in four sub-industries following set ups of baseline analysis. ***, **, and * indicate the subsamples are significantly different from each other at the 1%, 5%, and 10% levels, respectively.

Panel A: Baseline analysis

	Market model	Fama–French 3 Factor model
	(1)	(2)
[-3,3]	-0.0193**	-0.0171*
	(-2.03)	(-1.84)
Observations	65	65

Panel B: Robustness test

	Market model	Fama–French 3 Factor model	Fama–French 4 Factor model
	(1)	(2)	(3)
[-2,2]	-0.0129*	-0.0128*	
	(-1.77)	(-1.82)	
[-3,3]			-0.0227**
			(-2.43)
Observations	65	65	65

Panel C: CARs separated by sub-industry

	Airline (1)	Hotel (2)	Restaurant (3)	Casino (4)
Market model	0.0489**	-0.0360**	-0.0254*	0.0251*
	(2.22)	(-2.43)	(-1.76)	(1.66)
Fama–French 3 Factor model	0.0506	-0.0325**	-0.0228*	0.0209
	(1.63)	(-2.35)	(-1.87)	(1.35)
Observations	5	31	22	7

Table 4 Spillover effect of Data Breach

This table presents the OLS regressions of spillover effects of data breaches to sub-industries. Regressions include year fixed effects and firm fixed effects. ***, **, and * indicate the subsamples are significantly different from each other at the 1%, 5%, and 10% levels, respectively.

	Market model	Fama–French 3 Factor model
	(1)	(2)
SPILLOVER_HOTEL	-0.0154***	-0.0112**
	(-3.23)	(-2.40)
SPILLOVER_REST	-0.0201***	-0.0224***
	(-3.66)	(-4.09)
BM	0.0057	0.0047
	(1.41)	(1.20)
ROA	0.0334	0.0312
	(1.37)	(1.28)
Size	0.0014	0.0013
	(0.40)	(0.38)
Constant	-0.0183	-0.0157
	(-0.73)	(-0.64)
Observations	5,691	5,691
R-squared	0.209	0.215
Year FE	YES	YES
Firm FE	YES	YES
Adj./Pseudo R2	0.167	0.174

Table 5: Heterogeneity test

This table presents OLS regressions of heterogeneity tests. Regressions include year fixed effects and firm fixed effects. Panel A reports the influence of customer information leakage on spillover effect. Panel B reports the impact of the number of data affected on spillover effect. Panel C reports the result of data breach firm size on the spillover effect. Panel D reports the result of data breach occurrence on the spillover effect. ***, **, and * indicate the subsamples are significantly different from each other at the 1%, 5%, and 10% levels, respectively.

Panel A: Customer information leakage

	Market model	Fama–French 3 Factor model
	(1)	(2)
SPILLOVER_HOTEL	0.0041	0.0048
	(0.68)	(0.79)
SPILLOVER_REST	-0.0214***	-0.0251***
	(-3.02)	(-3.59)
SPILLOVER_HOTEL × Customer	-0.0264***	-0.0240**
	(-2.60)	(-2.37)
SPILLOVER_REST × Customer	0.0176	0.0133
	(1.56)	(1.19)
Customer	-0.0285***	-0.0212***
	(-6.16)	(-4.85)
BM	0.0080*	0.0070
	(1.73)	(1.54)
ROA	0.0319	0.0312
	(1.35)	(1.32)
Size	-0.0001	-0.0001
	(-0.04)	(-0.03)
Constant	-0.0024	-0.0025
	(-0.09)	(-0.10)
Observations	5,300	5,300
R-squared	0.249	0.248
Year FE	YES	YES
Firm FE	YES	YES
Adj./Pseudo R2	0.207	0.206

Panel B: Affected data disclosure

	Market model	Fama–French 3 Factor model
	(1)	(2)
SPILLOVER_HOTEL	-0.0065	-0.0015
	(-1.11)	(-0.26)
SPILLOVER_REST	-0.0395***	-0.0413***
	(-4.75)	(-4.96)
SPILLOVER_HOTEL × Disclose	0.0064	0.0043
	(0.60)	(0.42)
SPILLOVER_REST ×Disclose	0.0450***	0.0439***
	(4.05)	(3.99)
Disclose	-0.0401***	-0.0423***
	(-9.72)	(-10.75)
BM	0.0081*	0.0070
	(1.75)	(1.57)
ROA	0.0319	0.0320
	(1.33)	(1.34)
Size	0.0002	0.0002
	(0.04)	(0.06)
Constant	-0.0017	-0.0007
	(-0.07)	(-0.03)
Observations	5,300	5,300
R-squared	0.252	0.259
Year FE	YES	YES
Firm FE	YES	YES
Adj./Pseudo R2	0.210	0.217

Panel C: Breached firm size

	Market model	Fama–French 3 Factor model
	(1)	(2)
SPILLOVER_HOTEL	-0.0078*	-0.0071
	(-1.84)	(-1.64)
SPILLOVER_REST	-0.0270***	-0.0322***
	(-3.30)	(-4.00)
SPILLOVER_HOTEL × *SizeD*	0.0153	0.0190*
	(1.36)	(1.72)
SPILLOVER_REST × *SizeD*	0.0375***	0.0379***
	(3.26)	(3.36)
SizeD	-0.0543***	-0.0484***
	(-10.99)	(-10.42)
BM	0.0077*	0.0067
	(1.69)	(1.50)
ROA	0.0353	0.0352
	(1.46)	(1.47)
Size	0.0004	0.0004
	(0.11)	(0.11)
Constant	-0.0019	-0.0017
	(-0.07)	(-0.07)
Observations	5,300	5,300
R-squared	0.259	0.259
Year FE	YES	YES
Firm FE	YES	YES
Adj./Pseudo R2	0.217	0.217

Panel D: Data breach occurrence

	Market model	Fama–French 3 Factor model
	(1)	(2)
SPILLOVER_HOTEL	0.0173	0.0198
	(1.37)	(1.58)
SPILLOVER_REST	-0.0084	-0.0086
	(-1.20)	(-1.24)
SPILLOVER_HOTEL × Repeat	-0.0295**	-0.0289**
	(-2.13)	(-2.10)
SPILLOVER_REST × Repeat	0.0004	-0.0082
	(0.04)	(-0.75)
Repeat	-0.0192***	-0.0140***
	(-5.24)	(-4.01)
BM	0.0095*	0.0086*
	(1.88)	(1.75)
ROA	0.0414	0.0411
	(1.46)	(1.45)
Size	-0.0001	-0.0001
	(-0.03)	(-0.04)
Constant	-0.0044	-0.0038
	(-0.15)	(-0.14)
Observations	5,025	5,025
R-squared	0.234	0.241
Year FE	YES	YES
Firm FE	YES	YES
Adj./Pseudo R2	0.190	0.197

Table 6: Data breaches and cash holdings

This table presents the results of the OLS regressions. All variables are defined in the Table 1. All independent variables are measured at t−1 for estimating the regression. All continuous variables are winsorized at the 1% level at both tails of their distributions. The regressions include firm and year fixed effects. ***, **, and * indicate significance at the 1%, 5%, and 10% levels, respectively.

Panel A Effects of data breaches to focal firm's cash holdings

	Full sample	Sub-industry	
		Hotel	Other 3
VARIABLES	*CASH*	*CASH*	*CASH*
	(1)	(2)	(3)
DATABREACH	0.0684**	0.1597***	-0.0148
	(2.11)	(3.19)	(-1.09)
BM	0.2063***	0.1062	0.0617***
	(4.72)	(1.07)	(2.72)
LEV	-0.0191	0.4078***	-0.0871**
	(-0.43)	(3.41)	(-2.22)
Size	-0.2828***	-0.1058*	-0.1962***
	(-7.29)	(-1.87)	(-6.27)
Net Working Capital	-0.1935	-1.0248***	0.4208
	(-0.66)	(-2.97)	(1.31)
CFO	-1.7837***	-1.9891***	-0.6323***
	(-7.43)	(-4.59)	(-3.81)
CFOVAR	11.0812***	11.4258**	5.8967***
	(5.53)	(2.54)	(3.83)
INVEST	0.2842	-0.829	-0.5761***
	(1.05)	(-0.93)	(-3.21)
Z_SCORE	0.0444	0.0481	-0.0359
	(0.94)	(0.70)	(-0.81)
Constant	2.7022***	1.0372*	1.9599***
	(7.54)	(1.84)	(6.84)
Observations	1,117	397	720
R-squared	0.552	0.638	0.627
Year FE	YES	YES	YES
Firm FE	YES	YES	YES
Adj./Pseudo R2	0.529	0.605	0.602

Panel B Effects of data breaches to cash holdings of firms in the same sub-industry

	Full sample	Sub-industry	
		Hotel	Other 3
	CASH	*CASH*	*CASH*
	(1)	(2)	(3)
SPILL	0.0267**	0.1054*	0.0178***
	(2.54)	(1.88)	(2.70)
BM	-0.0115	-0.0733**	-0.0148
	(-0.93)	(-2.12)	(-1.41)
LEV	-0.0656**	0.3321	-0.0394*
	(-2.16)	(1.14)	(-1.69)
Size	0.0163	-0.0651	-0.0054
	(0.92)	(-1.58)	(-0.37)
Net Working Capital	-0.0148	0.2645	0.0183
	(-0.14)	(0.56)	(0.22)
CFO	-0.8259***	-1.7996***	-0.4570***
	(-6.10)	(-3.15)	(-5.24)
CFOVAR	1.8975***	4.8787	0.7165
	(2.79)	(1.43)	(1.47)
INVEST	0.2881**	-1.298	0.0647
	(2.11)	(-1.05)	(0.65)
Z_SCORE	0.0268	0.0667	0.0462*
	(0.83)	(1.06)	(1.86)
Constant	0.2134	1.2882***	0.2782***
	(1.64)	(4.19)	(2.69)
Observations	3,988	530	3,457
R-squared	0.701	0.725	0.646
Year FE	YES	YES	YES
Firm FE	YES	YES	YES
Adj./Pseudo R2	0.684	0.695	0.625

Panel C Effects of data breaches to cash holdings of firms across the sub-industry

	Hotel	Restaurant	Casino	Airline
	CASH	*CASH*	*CASH*	*CASH*
	(1)	(2)	(3)	(4)
SPILL_OTHERS	0.0256***	-0.0030	-0.0247*	-0.0109
	(3.15)	(-0.13)	(-1.68)	(-0.37)
BM	-0.0147	0.0047	-0.0108	-0.0033
	(-1.41)	(0.14)	(-1.60)	(-0.31)
LEV	-0.0391*	-0.0004	-0.0993***	-0.0460
	(-1.68)	(-0.00)	(-3.34)	(-1.48)
Size	-0.0053	-0.0352	0.0399**	0.0153
	(-0.36)	(-1.20)	(2.53)	(0.80)
Net Working Capital	0.0180	-0.0518	0.1898*	-0.1705
	(0.21)	(-0.27)	(1.71)	(-1.46)
CFO	-0.4557***	-1.7924***	-0.7331***	-0.7673***
	(-5.22)	(-5.55)	(-5.44)	(-5.09)
CFOVAR	0.7211	0.5363	0.9081*	2.7624***
	(1.48)	(0.33)	(1.76)	(3.20)
INVEST	0.0680	0.2933	0.3704***	0.3806**
	(0.68)	(0.97)	(3.08)	(2.31)
Z_SCORE	0.0458*	0.1955***	-0.0661***	0.0431
	(1.84)	(3.28)	(-2.80)	(1.62)
Constant	0.2771***	0.8217***	0.1114	0.2007
	(2.69)	(3.30)	(0.95)	(1.49)
Observations	3,457	2,150	3,024	3,333
R-squared	0.647	0.667	0.745	0.701
Year FE	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES
Adj./Pseudo R2	0.626	0.645	0.729	0.683

Table 7: Data breaches and dividend payouts

This table presents the results of the OLS regressions. All variables are defined in the Table 1. All independent variables are measured at t−1 for estimating the regression. All continuous variables are winsorized at the 1% level at both tails of their distributions. The regressions include firm and year fixed effects. ***, **, and * indicate significance at the 1%, 5%, and 10% levels, respectively.

Panel A Effects of data breaches to focal firm's dividend payouts

	Full sample	Sub-industry	
		Hotel	Other 3
	DPS	*DPS*	*DPS*
	(1)	(2)	(3)
DATABREACH	-0.1556**	-0.2578**	-0.0273
	(-2.13)	(-2.36)	(-0.35)
Size	0.0390	0.1049	-0.2659***
	(0.45)	(0.42)	(-3.12)
ROA	4.1575***	10.8904***	1.3378***
	(5.60)	(5.40)	(3.07)
CASH	0.3001*	1.6083***	0.1815
	(1.96)	(5.37)	(0.88)
BM	-0.0570	-0.4343**	0.3690**
	(-0.42)	(-2.15)	(2.37)
LEV	0.5241***	-3.4936***	0.6659**
	(3.03)	(-5.07)	(2.53)
Tangibility	1.1042***	-2.5776***	0.3330
	(3.28)	(-2.91)	(1.06)
Volatility	-0.5367	2.1656*	0.0552
	(-1.09)	(1.71)	(0.10)
Age	0.2268	1.8441***	0.1533
	(0.95)	(4.92)	(0.40)
Constant	-1.3295	-4.4278	1.6791
	(-1.05)	(-1.60)	(1.10)
Observations	1,176	458	718
R-squared	0.762	0.688	0.867
Year FE	YES	YES	YES
Firm FE	YES	YES	YES
Adj./Pseudo R2	0.750	0.663	0.859

Panel B Effects of data breaches to dividend payouts of firms in the same sub-industry

	Full sample	Sub-industry	
		Hotel	Other 3
	DPS	*DPS*	*DPS*
	(1)	(2)	(3)
SPILL	0.0197	0.0075	0.0239
	(0.77)	(0.64)	(0.77)
Size	-0.0460**	-0.0430***	-0.0367
	(-1.98)	(-3.18)	(-1.01)
ROA	0.6466***	0.0889	0.8656***
	(7.35)	(1.37)	(7.94)
CASH	0.0217	-0.0237**	-0.0298
	(0.96)	(-2.24)	(-0.69)
BM	0.0371***	-0.0049	0.0502***
	(2.87)	(-0.37)	(3.17)
LEV	0.2618***	-0.2168***	0.3283***
	(3.10)	(-2.95)	(3.64)
Tangibility	0.1389	-0.1902	0.1732
	(1.20)	(-1.31)	(1.27)
Volatility	-0.6622***	-0.3246**	-0.6274***
	(-3.60)	(-2.41)	(-2.84)
Age	0.2636***	0.1365**	0.2197*
	(2.79)	(1.97)	(1.80)
Constant	-0.2225	0.3583**	-0.2274
	(-0.78)	(2.13)	(-0.57)
Observations	4,231	698	3,532
R-squared	0.585	0.823	0.580
Year FE	YES	YES	YES
Firm FE	YES	YES	YES
Adj./Pseudo R2	0.559	0.806	0.555

Panel C Effects of data breaches to dividend payouts of firms across the sub-industry

	Hotel	Restaurant	Casino	Airline
	DPS	*DPS*	*DPS*	*DPS*
	(1)	(2)	(3)	(4)
SPILL_OTHERS	0.0382	-0.0000	-0.0260	-0.1015
	(1.56)	(-0.00)	(-0.95)	(-1.61)
Size	-0.0367	0.0790***	-0.1264***	-0.0537**
	(-1.01)	(3.56)	(-4.26)	(-2.28)
ROA	0.8632***	0.5568***	0.6244***	0.5260***
	(7.92)	(4.35)	(6.48)	(6.01)
CASH	-0.0321	0.0070	0.0757**	0.0150
	(-0.75)	(0.50)	(2.51)	(0.66)
BM	0.0501***	-0.0390***	0.0377***	0.0247**
	(3.16)	(-2.88)	(3.34)	(2.03)
LEV	0.3288***	-0.1349*	0.3172***	0.1730*
	(3.64)	(-1.65)	(3.30)	(1.86)
Tangibility	0.1719	0.5622***	0.1392	0.0000
	(1.27)	(5.78)	(0.90)	(0.00)
Volatility	-0.6537***	-0.3096*	-0.9065***	-0.7380***
	(-2.95)	(-1.84)	(-4.16)	(-3.80)
Age	0.2197*	0.2583***	0.4232***	0.2621**
	(1.80)	(3.44)	(3.74)	(2.44)
Constant	-0.2258	-1.2322***	-0.0681	-0.0009
	(-0.56)	(-5.15)	(-0.20)	(-0.00)
Observations	3,532	2,398	3,231	3,532
R-squared	0.580	0.553	0.618	0.594
Year FE	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES
Adj./Pseudo R2	0.555	0.523	0.595	0.568