The Impact of Data Breaches on Hotel and Restaurant Firm Stock Returns

THE JOURNAL OF HOSPITALITY FINANCIAL MANAGEMENT
2018, VOL. 26, NO. 2, 75–86
https://doi.org/10.7275/v8kg-hy29

The Impact of Data Breaches on Hotel and Restaurant Firm Stock Returns

Mark S. Johnson
Eli Broad College of Business, Michigan State University, East Lansing, MI

Min Jung Kang
School of Management, University of Michigan–Flint, Flint, MI

Tolani Lawson
Senior Financial Analyst, WestRock Company, Lansing, MI

A. J. Singh
College of Business and Entrepreneurship, University of Texas Rio Grand Valley, Brownsville, TX

ABSTRACT
Hospitality firms are susceptible to data breaches due to the high volume of information they keep on customers and employees. In this paper, we first present an analysis of the stock market's reaction to data breaches at hospitality firms, and we compare these breaches to a matched-firm sample of retail firm breaches. Abnormal stock market returns indicate that hotel and restaurant firm stock prices went down by approximately 1.24% from data breach announcements. We find that the type of breach or number of times a firm has been breached does not alter the impact of a breach on firm returns. Additionally, we find that data breaches cause a greater loss of value for hotel firms than for restaurants. Finally, we find no support for the idea that hospitality firms exhibit larger negative effects compared to retail firms on a matched-pair analysis.

Keywords: *CAPM, data breach, event study, stock returns*

1 Introduction and Study Context

Organizations of all types have become increasingly susceptible to data breaches, and data breaches, via hacking and other exposures, are growing more common. Breaches are leading to more costs, occasional fines, and more claims being paid out as the cyber liability market matures. The Ponemon Institute's 2015 study, *Cost of data breach: Global analysis*, found that German and U.S. companies experienced the highest total cost of data breaches, with the U.S. at $5.4 million, on average, in 2013.

Data breaches occur in many forms, which include hacking, stolen or lost equipment, and poor data handling processes. Hotels and restaurants are not exempt from this increasing trend, and they may be more susceptible to data breaches because of the volume of information residing in their systems, including credit card data, confidential information for loyalty programs, and employee data. Easy access to wireless networks, the use of physical point-of-sale devices within hotel restaurants and bars, and a multitude of employees with access to guest information all increase the risk. According to a data breach investigation conducted by SpiderLabs's 2015 Trustwave Global Security Report, criminals go after the food and beverage industry because it tends to have high transaction volumes. Criminals have found that these organizations have a low barrier to entry from an infiltration standpoint. SpiderLabs's 2015 report found that the hospitality and food and beverage industry formed 33% of the primary targets of cyber criminals in 2012. Additionally, a study reported in *Hospitality Technology* (2017) indicated that 74% of hotels do not have data breach protection. In this same article John Bell,

CONTACT: Address correspondence to Mark S. Johnson, Eli Broad Graduate School of Management, Michigan State University, 324 Eppley Center, East Lansing, MI 48824, USA. Email: johnsonm@broad.msu.edu.

founder of the security consulting firm Ajontech LLC, stated that "hackers love hospitality." Thus, it seems that hospitality firms may have higher data breach costs and exposure compared to other retail firms. Additionally, it is unclear within the hospitality industry whether hotels or restaurants have greater value and risk exposure to data breaches. This is because two possibly offsetting effects exist. Hotels, because of their low level of preparedness, may be worse off than restaurant firms. On the other hand, restaurants have a very high rate of transactions and may be more exposed to data breach loss than hotel firms. If a difference exists, it is unclear which type of firm will suffer a greater decline in value from a data breach.

The true cost of a data breach is not limited to the financial consequences of lost business and exposure to third party liability; there are also risks related to reputation ranging from significant to catastrophic. This paper analyzes the consequences of data breach incidents in hotel and restaurant firms: the effect of the announcement of data breaches on stock value. Previous studies have looked at the effect of data breaches on different groups of firms. This paper is the first to examine a sample of events consisting exclusively of firms in the hospitality industry. This paper aims to identify the economic importance of data breaches in the hospitality industry from an investor's viewpoint.

1.1 Outline of the Paper

Our paper proceeds as follows. Section 2 reviews the literature and provides the paper's hypotheses. Section 3 explains the research design for the event study portion of the paper and describes the sample firms used in our event study, event study methodology, and the firm and breach characteristics that affect the abnormal return of the firms. Results of the event study are presented in Section 4. Section 5 summarizes the findings and contributions of the research.

2 Previous Event Studies in Hospitality Finance

The usefulness of event study methodology is well-established in hospitality literature. Previous event studies have examined a variety of factors that may impact shareholder value in the hospitality industry including: initial public offerings (Canina, 1996), acquisitions (Canina, 2001; Ma & Chowdry, 2011), terrorism (Chang & Zeng, 2011), travel promotion (Johnson, Singh, & Ma, 2015), federal tax policy (Johnson & Johnson, 2016), etc. There are no published papers in hospitality literature that have used event study methodology to examine the impact of data breaches on firm value. However, there are numerous examples of event studies outside the hospitality literature that have examined the effects of data breach on other industries.

The implicit assumption in this methodology is that the financial markets respond to news that affect a security's value, so change in stock price is a good proxy for the impact of a given event. The event study methodology assumes that returns on a stock are significantly impacted by an event of interest. Overall, previous studies found that the market discriminates breached companies in the first few days following the public announcement of the breach.

However, no previous studies have investigated the impact of security breaches on hospitality firms. This study considers the impact of data breaches on hospitality firm values. Additionally, the study compares the hospitality firm data breaches to a matched-pair set of retail firm data breaches.

2.1 Literature Review of Data Breach Event Studies and Possible Factors Impacting the Size of Abnormal Returns

The results in event study literature that examine data breaches and firm value provide mixed and possibly contradictory results. Some studies found significant negative firm value effects associated with data breaches and some did not. Some studies found that malicious data breaches, hacking, cause more harm and other studies did not. Finally, one study found that a repeat data breach is more detrimental to firm value and some did not. For a summary of the results of previous event studies, see Table 1 below. The studies in Table 1 all utilized the capital asset pricing model to determine the abnormal returns associated with data breach information reaching the marketplace. Studies vary in size from 22 firm breach events over a 7-year period to 467 breach events over a 10-year period.

Table 1. Summary of Previous Data Breach Event Studies

Author	Publication Date	Sample Size	Category of Firm Type	Data Years	Window	CAAR Entire Sample	Hacking More Negative?[1]	Repeat More Negative?[1]
Acquisti et al.	2006	79	Broad Sample	2000–2006	2-day	−0.58%	No	N.A.
Campbell et al.	2003	43	Broad Sample	1995–2000	3-day	Not Significant	Yes	N.A.
Cavusoglu et al.	2004	66	Broad Sample	1996–2001	2-day	−2.1%	No	N.A.
Garg et al.	2003	22	Denial Of Service Attacks (Hacking)	1996–2002	3-day	−5.3%	N.A.	N.A.
Gatzlaff et al.	2010	77	Broad Sample	2004–2006	2-day	−0.46%	No	Yes
Hovav et al.	2003	23	Internet Only Firms	1998–2002	3-day	Not Significant	N.A.	N.A.
Johnson et al.	2017	467	Broad Sample	2005–2014	3-day	−0.37%	No	No
Kannan et al.	2004	102	50% Viruses	1998–2002	4-day	Not Significant	No	No

1. N.A. is defined as not applicable. Many of the previous studies did not examine the possibility that hacking or repeat breaches are more destructive to firm value.

Five of the eight studies examined a broad range of breach types across many industries (Acquisti, Friedman, & Telang, 2006; Campbell, Lawrence, Loeb, & Zhou, 2003; Cavusogul, Mishra, & Raghunathan, 2004; Gatzlaff & McCullough, 2010; Johnson, Kang, & Lawson, 2017). In these broad-sample based studies the results range from 0 to −2.1%. Johnson et al. (2017), with the largest sample size of 467, reported a −0.37% return associated with the average data breach. The preponderance of the evidence seems to indicate that the average data breach is bad news for a firm's value but is of modest economic significance.

Of the three studies that are not broad based, the one that may be of greatest interest here is the Garg, Curtis, and Harper (2013) study that found, for a sample of denial of service hacks, there is a very large significant −5.3% abnormal return. Denial of service is a type of hacking where the hacker degrades the ability of the corporation to serve customers and other stakeholders through their IT services and websites. This includes but is not limited to slowing down the firm's website, stopping legitimate access through viruses, etc. This result is much more severe than that reported in all other studies. In general agreement with this result, Campbell et al. (2003) found in their broad sample of firms that hacking breaches are significantly more negative than other data breaches. On the other hand, Johnson et al. (2017); Kannan, Rees, and Sridhar (2011); and Gatzlaff and McCullough (2010) found that hacking events are not more deleterious to firm value. Thus, it is unclear from the previous evidence whether breach type impacts the size of the returns associated with the data breach.

The final two studies, Kannan et al. (2011) and Hovav and D'Arcy (2003), were based on relatively narrow samples of breaches. In the Kannan et al. (2011) study 50% of the breaches were viruses attacking the company's computer system. These virus attacks can be viewed as a type of hacking event. To put this in perspective, only 22% of the data breaches in the Johnson et al. (2017) study of 467 breaches were hacking events. The Hovav and D'Arcy (2003) study was limited to the examination of Internet firms. Because of the limited scope of these studies it is difficult to obtain reasonable inferences for the average publicly traded firm or the hospitality industry.

Several of the studies went on to examine whether a repeat data breach has a different impact on a firm's value than an original event. Here a repeat breach is described as a second, third, or subsequent breach experienced by a firm within the timespan of the study. Hence a breach that is described in a study as a first breach could in fact be a repeat breach in that an earlier breach occurred prior to the horizon of the study. Gatzlaff and McCullough (2010) found that repeat breaches do cause a more negative response to breaches than first-time events. The Gatzlaff study was based on 77 breach events over a

three-year period. On the other hand, Johnson et al. (2017), with a broad-based sample of 467 breaches, and Kannan et al. (2011), with a narrow sample, both found no greater negative effect for repeat breaches. Therefore, the evidence, while inconclusive, leans in the direction of finding no repeat effect.

The issues investigated in this paper arise from the discussion of Section 1, the introduction to the paper, and Section 2.1, previous event study results. Two sets of issues will be addressed. The first issue is determining the average impact of a data breach on hospitality firms. The hypothesis for this issue is presented in Section 2.2 below. The second set of issues asks whether some types of data breaches, or types of firms, create a different abnormal return than others. In Section 2.3 below there are two hypotheses that examine types of data breaches. The first breach type is malicious data breaches (MAL), which include hacking and insiders misusing data. The second type is repeat (REPEAT) data breaches. In Section 2.3 there are also two hypotheses that examine whether firm type matters. The first of these hypotheses examines whether restaurants are differentially impacted compared to hotels. The last hypothesis addresses whether hospitality firms are uniquely worse off in comparison to other retail firms.

2.2 Market Reaction to Data Breaches

The first goal of this paper is to discover the extent to which data breaches impact the value of firms in the hospitality industry. The previous literature seems to indicate that the overall impact on firms experiencing data breaches is either negative or zero. Five of the eight studies found a significant negative effect associated with data breaches and three did not. Hence, our first hypothesis, stated in the null, becomes:

H1: There is no average abnormal stock market reaction to reports of corporate data breaches in hotels and restaurants.

2.3 Cross-Sectional Determinants of Market Reaction

We also develop four hypotheses about how the impact of a data breach on a given firm will vary with the firm's competitive situation and the characteristics of the data breach. The first competitive factor is based on the nature of the security breach. We identify five types of data breaches across our sample of hotel and restaurant data breach events. These data breach types are listed in Panel B of Table 2 and include insider (INSD), unintended disclosure (DISC), physical loss (PHYS), hacking or malware (HACK), and portable device (PORT). Two of these types of data breaches, INSD and HACK, are based on malicious acts. Insiders that have legitimate access to data but inappropriately release that data (INSD) are engaging in a malicious act. Similarly, hacking or malware attacks (HACK) are malicious acts in which an external party, through malware or spyware, seeks and exploits weaknesses in a computer system or computer network. One previous study found that malicious breaches are more disruptive than other breaches and five studies found no evidence of a differential effect.

Thus, stated in the null, our hypothesis becomes:

H2a: Ceteris paribus, the magnitude of abnormal negative returns that result from MAL breaches will not differ from all other types of breach.

The second factor that may influence the magnitude of the impact from a data breach is a repeated occurrence. One previous study found that repeat breaches were more negative than original breaches, but two studies found no difference. If negative abnormal returns are greater for firms experiencing multiple breaches during the time frame examined in our sample, it may suggest that investors react more strongly to firms that fail to take appropriate measures to protect sensitive information after a breach incident occurs for the first time.

Thus, stated in the null, our hypothesis becomes:

H2b: Ceteris paribus, the magnitude of abnormal negative returns due to a privacy breach is not different for events that are a repeated occurrence of a privacy breach.

The third factor that we consider is the magnitude of the impact of a data breach on hotel firms compared to restaurant firms. The Verizon 2012 data breach investigation report showed that the most

Table 2. Sample Firms and Data Breach Types

PANEL A: Hospitality Firm Names, Breach Dates, Ticker, and Type of Breach

Breach Event	Company Name	Original Event Date	Ticker	Type of Breach	Mkt Cap in Billions
1	Flanigans Enterprises, Inc.	05/20/2011	BDL	INSD	0.05
2	Cheesecake Factory, Inc.	05/24/2010	CAKE	INSD	2.30
3	Cheesecake Factory, Inc.	09/13/2010	CAKE	INSD	2.30
4	Cheesecake Factory, Inc.	09/29/2010	CAKE	INSD	2.30
5	Choice Hotels International, Inc.	04/26/2012	CHH	DISC	3.28
6	Denny's Corp.	09/30/2013	DENN	PHYS	0.85
7	Domino's Pizza, Inc.	06/18/2008	DPZ	PHYS	5.22
8	Starwood Hotels	03/08/2010	HOT	HACK	14.56
9	Jack In The Box, Inc.	02/22/2011	JACK	INSD	2.92
10	Marriott International, Inc. New	12/28/2005	MAR	PORT	22.38
11	Marriott International, Inc. New	02/07/2011	MAR	PHYS	22.38
12	McDonald's Corp.	12/14/2010	MCD	HACK	93.73
13	McDonald's Corp.	08/09/2011	MCD	INSD	93.73
14	McDonald's Corp.	09/12/2011	MCD	INSD	93.73
15	McDonald's Corp.	11/07/2011	MCD	INSD	93.73
16	McDonald's Corp.	11/16/2011	MCD	INSD	93.73
17	McDonald's Corp.	03/09/2012	MCD	INSD	93.73
18	McDonald's Corp.	04/30/2012	MCD	INSD	93.73
19	McDonald's Corp.	02/07/2013	MCD	INSD	93.73
20	Papa John's Intl, Inc.	11/07/2005	PZZA	DISC	2.17
21	Starbucks Corp.	11/03/2006	SBUX	PORT	62.54
22	Starbucks Corp.	11/24/2008	SBUX	PORT	62.54
23	Wyndham Worldwide Corp.	02/16/2009	WYN	HACK	10.46
24	Wyndham Worldwide Corp.	03/01/2010	WYN	HACK	10.46

PANEL B: Description of Type of Breaches Observed in Hospitality Firms

Data Breach Type	
DISC	Unintended disclosure: Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail.
HACK	Hacking or malware: Electronic entry by an outside party, malware and spyware that is malicious in nature.
INSD	Insider: Someone with legitimate access intentionally breaches information, such as an employee or contractor with malicious intent.
PHYS	Physical loss: Lost, discarded, or stolen non-electronic records, such as paper documents.
PORT	Portable device: Lost, discarded, or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
REPEAT	A proxy for breaches that represent a repeated occurrence for the individual firm within the time frame of the study.

reported data breach incidents in 2012 were from accommodation and food services, and around 95% of these were restaurants while the remaining 5% were hotels. On the other hand, as discussed in the introduction, hotels may be less prepared for data breaches than restaurant firms. Thus, the value exposure of restaurants and hotels may be significantly different in either direction.

H2c: Ceteris paribus, the magnitude of abnormal negative returns is not significantly different in hotels than in restaurants.

Lastly, we compare the magnitude of abnormal negative returns in the hospitality industry with that of the retail industry off-sample that consists of breaches with similar breach types and firm size as the sample of hospitality breaches. While we do not have a study that specifically suggests this hypothesis, we do have a statement from John Bell in *Hospitality Technology* (2017) that "hackers love hospitality." This seems to suggest that hospitality firms may be more heavily exposed to data breaches than other retail consumer-oriented activities. Thus, stated in the null, our hypothesis becomes:

H2d: Ceteris paribus, the magnitude of abnormal negative returns is not different for a set of matched-pair retail firms as compared to hospitality firms.

3 Event Study Research Design

This section discusses the data and research design used in the study.

3.1 Sample Firms

The sample used for this study consists of instances of data breaches that publicly traded entities in the hospitality industry have been susceptible to in the past 10 years. The list of breaches appears in Table 2. This sample was derived by collecting a list of all data breaches from the last 10 years from Privacy Rights Clearinghouse. We chose this medium for selecting our sample because we wanted to develop a sample that was representative of the sum of information security breaches. Our search for information security breaches covers the period of January 2005 through December 2014. The raw dataset obtained from Privacy Rights Clearinghouse contained 1,715 data breach events in sectors including business, educational institutions, government/military, health care/medical providers, and nonprofit organizations. Privacy Rights Clearinghouse obtains its lists through federal and state government reports, reports in major newspapers, and online reports of data breaches. This list was sorted for publicly traded companies in the United States that operate in the restaurant and hotel business. This narrowed our initial selection down to 31 data breach events and 15 unique publicly listed U.S. firms.

Additional sample selection criteria are the availability of sufficient returns history (i.e., a minimum public trading history) from the Center for Research in Security Prices (CRSP) database for the estimation period necessary for our event study, continuity in the corporate entity's identity over the period, and elimination of multiple events where estimation periods overlap earlier events for the same firm.[1] Seven events were eliminated, leaving us with 24 observations and 13 unique publicly listed U.S. firms in the hotel and restaurant business.

Two of the events that were eliminated from the initial sample selection were due to the unavailability of sufficient returns history on the CRSP database. These data breach events are the Burger King Worldwide, Inc. (BKW) insider breach on February 27, 2012[2] and the Las Vegas Sands Corp. (LVS) hacking on February 12, 2014.[3] Another two events were eliminated due to confounding occurrences around the data breach event date. The first firm, Domino's Pizza, Inc. (DPZ), had a data breach on May 12, 2011, and made several significant announcements around this period. On April 27, 2011, Domino's Pizza, Inc. announced the acquisition of a majority stake in the exclusive master franchise to own, operate, and franchise Domino's Pizza stores in Germany. On May 5, 2011, the group announced its first quarter results and on May 18, 2011, it was awarded the "chain of the year" award for the third time back-to-back. The second firm, Wyndham Worldwide Corp. (WYN), had a data breach on June 12, 2013, that was eliminated due to a Florida law that protected timeshare owners signed on June 13, 2013. Wyndham Vacation Ownership, a member of Wyndham Worldwide's family companies, as reported in a 2013 press release, is the world's largest vacation ownership business as measured by the number of vacation ownership resorts, individual vacation ownership units, and owners of vacation ownership interests.

Wendy's Company and McDonald's Corp. also had breach events that were eliminated from the sample. The Wendy's Company (WEN) had two events that had to be eliminated because the events occurred in 2007 and 2008 under the name Triarc Companies, Inc. and operated as a holding company for varied businesses. The last event eliminated was the McDonald's Corp. (MCD) data breach on November 18, 2011, because it overlapped with the event window of the data breach on November 16, 2011. Table 2 provides a list of the 24 events and the relevant firms, their ticker symbols, the date the data breaches were reported, and the type of breach.

[1] When there is an overlap in the estimation period with a prior event for the same firm, we use the earlier event reporting date.

[2] Burger King Holdings, Inc. (BKC) was delisted in October 2010 and then listed again in June 2012 as Burger King Worldwide, Inc.

[3] At the time of writing, there was no availability of sufficient returns history (i.e., a minimum public trading history) for the year 2014 in the CRSP database.

Table 3. One-to-One Matched Pair of Retail Firm

Off-Sample	PERMNO	Company Name	Original Event Date	Ticker	Type	Mkt Cap in Billions
1	84255	Seachange International, Inc.	09/08/2010	SEAC	INSD	0.27
2	91391	Windstream Corp.	01/27/2012	WIN	INSD	4.80
3	75489	Staples, Inc.	02/02/2012	SPLS	INSD	9.20
4	86580	Nvidia Corp.	01/13/2013	NVDA	INSD	12.32
5	89757	Sears Holdings Corp.	01/07/2008	SHLD	DISC	3.54
6	90396	Cubesmart	02/03/2012	CUBE	PHYS	4.08
7	46922	Rite Aid Corp.	07/27/2010	RAD	PHYS	5.52
8	85914	Best Buy Company, Inc.	05/06/2011	BBY	HACK	12.47
9	59010	GAP, Inc.	04/16/2010	GPS	INSD	17.27
10	39087	Sprint Nextel Corp.	01/22/2007	S	PORT	19.67
11	39917	Weyerhaeuser Co.	08/10/2006	WY	PHYS	18.01
12	25785	Ford Motor Co. Del	05/05/2012	F	HACK	65.51
13	12369	General Motors Corp.	08/03/2012	GM	INSD	60.95
14	19502	Walgreen Co.	03/11/2011	WAG	INSD	65.20
15	19502	Walgreen Co.	02/15/2013	WAG	INSD	65.20
16	19502	Walgreen Co.	12/20/2013	WAG	INSD	65.20
17	19502	Walgreen Co.	06/07/2014	WAG	INSD	65.20
18	77418	Time Warner, Inc. New	07/28/2010	TWX	INSD	71.71
19	17005	CVS Corp.	03/09/2011	CVS	INSD	104.82
20	10517	Aarons, Inc.	10/22/2013	AAN	DISC	2.11
21	89954	DirecTV Group, Inc.	10/11/2006	DTV	PORT	43.21
22	27828	Hewlett Packard Co.	12/11/2008	HPQ	PORT	60.54
23	89217	Advance Auto Parts, Inc.	03/31/2008	AAP	HACK	10.99
24	42585	Smucker J. M. Co.	03/04/2014	SJM	HACK	11.64

3.2 Off-Sample Firms

To compare the sample of hospitality firms to non-hospitality firms, an off-sample of retail firms were selected. A list of these off-sample, matched firms is provided in Table 3.

The off-sample consists of instances of data breaches that publicly traded entities in the retail industry have been susceptible to in the past 10 years. This sample was derived by collecting a list of all data breaches from the last 10 years from Privacy Rights Clearinghouse. The raw dataset obtained from Privacy Rights Clearinghouse contained 1,715 data breach events in sectors including business, educational institutions, government/military, health care/medical providers, and non-profit organizations. This list was then sorted for publicly traded companies in the United States that operate in the retail industry as defined by Privacy Rights Clearinghouse. Twenty-four matched events were selected such that the events were the same breach type and the nearest market capitalization (based on 2015 values) available as those in Table 2.

Additional sample selection criteria are the availability of sufficient returns history (i.e., a minimum public trading history) from the CRSP database for the estimation period necessary for our event study, continuity in the corporate entity's identity over the period, and elimination of multiple events where estimation periods overlap earlier events for the same firm.[1]

3.3 Test of Market Reaction

The first hypothesis is tested by examining the overall industry market reaction to the reporting date of each data breach event. The market reaction was determined by measuring daily abnormal returns (ARs), i.e., the difference between actual and expected returns. To control for the effects of market-wide fluctuations, the market model is used to measure expected returns:

$$R_{it} = \alpha_i + \beta_i R_{mt} + e_{it} \quad (1)$$

where:

R_{it} is the return for the ith data breach event on day t,

α_i is the intercept for the ith data breach event,

[1] When there is an overlap in the estimation period with a prior event for the same firm, we use the earlier event reporting date.

β_i is the slope coefficient for the *i*th data breach event,
R_{mt} is the return on an equal-weighted market portfolio on day *t*,
e_{it} is the error term with mean zero.

Following the conventions of previous studies (e.g. Hughes, Magat, & Ricks, 1986; Jarrell & Peltzman, 1985; and the findings of Brown & Warner [1980, pp. 242–243]; Brown & Warner [1985, p. 12]; and Binder & Summer [1985, p. 173]), an equal-weighted market index is used as a proxy for the market rate of return. The parameters α_i and β_i were estimated for the event by using 255 trading days of daily return data. Generally, in event studies, we want the parameters of the model to be estimated over a short time period before the event occurs. This involves a trade-off. The closer the estimation period is to the event period, the less likely it is that sample firm betas have changed due to changes in leverage, management strategy, and firm investments, etc. But estimation data from a period too close to the event period may be contaminated information leakage. We choose to estimate the parameters of the model using 255 days of data prior to each data breach event reporting date. We did this to, as much as possible, avoid confounding information about the data breach event that could potentially bias the estimates. Once the parameters α_i and β_i have been estimated for each firm, the daily prediction errors (abnormal returns) for firm *i* were calculated as follows:

$$AR_{it} = R_{it} - (\alpha_i + B_i R_{mt}) \tag{2}$$

where AR_{it} is the abnormal return for firm *i* on day *t*.

We examine abnormal returns for the three-day window that includes the event day and the two trading days immediately before and after the event. Inclusion of the trading day prior to the event controls for information leakage that may occur if some market participants are privy to the information prior to public announcement. Inclusion of the trading day after the event accounts for late arrival of information to the market or adjustment to information that requires time for market participants to interpret the true value effect of the data breach. A window that is too large will include extraneous information. Conversely, a window that is too small will not fully capture the effects of information leakage or slow market adjustment. We choose a window of three days. Thus, our results are reasonably conservative and should cover a significant amount of the impact of the data breach. Table 1 reveals that the choice of a three-day event window is similar to the event window length used in previous data breach event studies. Specifically, four of the previous reported studies use a three-day window with the remaining studies using either a two- or four-day window. The three-day cumulative abnormal returns for each firm was computed as below:

$$CAR_i = \sum_{t=-1}^{+1} AR_{\text{it}} \tag{3}$$

where

CAR_i is the cumulative abnormal return for data breach event *i*,
AR_{it} is the abnormal return for data breach event *i* on day *t*,
$t = 0$ is the day the data breach is reported to the government.

To determine the average overall impact of the events on the industry, we calculate the three-day cumulative average abnormal return by summing across the *n* firms in the sample and dividing by the number of firms in the sample as below:

$$CAAR = \sum_{i=1}^{24} CAR_i/24 \tag{4}$$

where

CAAR is the cumulative average abnormal return across all 24 events in the sample,
CAR_i is the three-day cumulative return for data breach event *i* around the event.

CAAR is the three-day cumulative average abnormal returns for the sample. To examine whether each informational event had a significant average return effect on the industry, a test of the null hypothesis that the three-day cumulative average abnormal

return across firms equals zero, for H1, is performed using Patel's Z-statistic.

3.4 Cross-Sectional Analysis and Matched-Pair Analysis of Competitive Factors

Cross-sectional analysis is employed to test the three hypotheses that differences in abnormal returns across firms are explained by underlying differences in the firms' competitive positions in terms of type of breach or whether the firm is a hotel or a restaurant. Specifically, multiple regression analysis is used to examine the relationship between each firm's market reaction to their respective data breach events and three characteristics that are predicted to explain some of the variation across data breach events.

The first explanatory variable is a dummy variable that equals one if the breach type is a malicious act (hack or insider misuse of data) and zero if it is not.

The second independent explanatory variable is a dummy that equals one if the breach is a repeat event for the firm involved and zero if it is not.

The third independent explanatory variable is a dummy variable that equals one if the firm involved in the breach is a restaurant and zero if it is a hotel.

We estimate the following multiple regression model for all available observations in the sample:

$$\text{Model:} \qquad (5)$$
$$CAR_i = \gamma_0 + \gamma_1 MAL_i + \gamma_2 REPEAT_i + \gamma_3 REST_i$$

where

CAR_i	is the three-day cumulative return for firm *i*,
MAL_i	is a dummy variable that equals one if the type of breach is malicious (hack or insider misuse of information),
$REPEAT_i$	is a dummy variable that equals one if the breach is a repeat event for the firm involved,
$REST_i$	is a dummy variable that equals one if the firm involved in the breach is a restaurant,
$\gamma_0, \gamma_1, \gamma_2, \gamma_3$	are the estimated intercept and three slope coefficients, respectively.

Our second and third coefficients represent a test of H2a that the estimated coefficient on *HACK,* $\gamma_{1,}$ will be zero, and H2b that the estimated coefficient on *REPEAT,* γ_2, will be zero. Our fourth coefficient is a test of the H2c hypothesis that predicts the estimated coefficient on REST, γ_3, will be zero. The results of the cross-sectional analysis are discussed in Section 4.2.

To test the last hypothesis, H2d, a matched-pair sample of comparable retail firms was selected based on our sample of hospitality firms. Based on extensive simulation results, Davies and Kim (2007) concluded that the best practice for constructing matched samples is to match firms one-to-one based on market capitalization and share price. Their results showed that tests based on one-to-one nearest-neighbor matching have comparable power and less size distortion than alternatives that place more weight on distant firms. We have used the following criteria to select a sample of one-to-one nearest-neighbor matching of retail firms: a) off-sample breach is for a retail firm as defined by Privacy Rights Clearinghouse, b) off-sample breach is a one-to-one match for the type of breach, c) off-sample breach after being matched by "a" and "b" is chosen as the firm breach such that the firm has the nearest possible firm size in terms of market capitalization at end of year 2015.

We then test the matched-pair sample by examining the overall industry market reaction to the reporting date of each data breach event. The market reaction was determined by measuring daily abnormal returns (ARs) in the same manner as discussed in Section 3.3. To control for the effects of market-wide fluctuations, the market model is used to measure expected returns:

$$R_{it} = \alpha_i + \beta_i R_{mt} + e_{it} \qquad (1)$$

Table 3 provides a list of the 24 matched-pair events and the relevant firms, their ticker symbols, the date the data breaches were reported, and the type of breach.

Finally, we compare via t-test (unequal variances), f-test, and Wilcoxon signed rank test the CARs on a matched-pair basis between the hospitality and retail firms to determine whether the two samples of breaches are similar.

4 Results

4.1 Results of Event Testing

Table 4 presents our test of hypothesis H1, which predicts that there is no effect on stock returns from data breaches.

CAAR, the cumulative average abnormal return, is an average of individual firm CARs.

$$CAAR = \sum_{i=1}^{24} CAR_{\mathrm{i}} \qquad (6)$$

where

$CAAR$ is the cumulative average abnormal return for the sample of 24 data breach events,
CAR_i is the cumulative abnormal return for data breach event i over the event window.

The CAAR for the hotel and restaurant data breaches in our sample is −1.24% at a level of significance of 0.062 for the Patel Z-Statistic. There are several different test statistics that are used in event studies. In other words, the equity values of our sample firms' equity reduced by an average of 1.24% in response to the data breaches. We find modest support for the conclusion that data breaches have a significant negative impact on the publicly traded hotel and restaurant firms in our sample.

Table 4. Cumulative Average Abnormal Return (CAAR) over a Three-Day Event Window around the Sample of 24 Data Breaches in Publicly Traded Hospitality Firms

Event Tested	Three-Day CAAR[1]	Pos/Neg[2]	Patel Z-Statistic (p-Value)[3]
Data Breaches	−1.24%	10/14	−1.539 (0.0620)

1. CAAR is the average abnormal return for the 24 event breaches in our sample over the three-day event window, day before, day of, and day after each data breach event. Abnormal returns are calculated using an equal weighted market index.
2. More of the firms had negative returns over the three-day event window.
3. The Patel Z-Statistic is generally recognized as the most appropriate test statistic for an event study of this type (Bloom, 2011). It is worth noting that a strict cutoff of 5% level of significance would have us not reject the null hypothesis. However, the authors think that 6% reflects general support for rejection of the null given the small sample size in the study.

4.2 Results of Cross-Sectional and Matched-Pair Analysis

Table 5 provides a summary of the results of a cross-sectional regression and hypothesis testing for H2a, H2b and H2c.

The findings do not reject the null hypotheses regarding MAL and REPEAT (at the 10% level). That is, malicious breaches and repeat breaches are no more, nor less, hurtful to hospitality firms. However, the coefficient on REST is positive and has a p-value of 0.056. It is reasonable to conclude that this provides modest evidence that restaurants are less negatively impacted by data breaches than hotels. This may be due to a lower level of preparedness on the part of hotels. This result seems to support the results of the study reported in *Hospitality Technology* (2017).

Table 6 presents our test of hypothesis H2d, which predicts that the stock price reaction to data breaches is different for hospitality firms as compared with off-sample matched retail firms.

The average abnormal return for the off-sample retail firms is −0.39% compared to −1.24% in the hospitality firms. However, the result is insignificant at the 10% level for all three tests examined. That is, to test the hypothesis three test statistics are provided a simple t-test (assuming unequal variances), an f-test, and a Wilcoxon signed rank test (non-parametric). The table reveals that all three tests are unable to reject the null hypothesis of equal means with a 10% level of significance. Therefore, despite the difference in means, −1.24% versus −0.39%, we are unable to claim that the two samples are significantly different. That is, hospitality firms are not impacted more, or less, heavily by data breaches than retail firms.

5 Summary, Conclusions, and Recommendations for Future Research

We examined the market reaction of hotel and restaurant firms to data breach events. The first result provided by the study is that there is modest evidence of a significant negative stock price effect from the average data breach. These negative effects may be attributed to current payments to customers associated with the breach and possible future declines in revenue from lost consumer confidence. The 1.24% negative cumulative abnormal

Table 5. Multiple Regression of Three-Day CAR_i[1] around the Sample of 24 Data Breach Events in Hotel and Restaurant Publicly Traded Firms

	Coefficients	Standard Error	t-Stat[5]	P-value
Intercept	−0.036793139	0.023025221	−1.597949468	0.125733901
MAL[2]	−0.02739201	0.02134573	−1.283254791	0.214073835
REPEAT[3]	0.015268288	0.019793064	0.771395859	0.449490894
REST[4]	0.045785871	0.022605273	2.025450966	0.056373842
R2 = 0.020764				
Regression Significance F = 0.189694378				

1. CAR_i is the three-day cumulative abnormal return for data breach event *i* around the date of reporting the data breach to the government.
2. MAL is a dummy variable that equals one if the type of breach is a malicious act such as a hack or an insider misuse of information and zero if it is not.
3. REPEAT is a dummy variable that equals one if the breach is a repeat event for the firm involved and zero if it is not.
4. REST is a dummy variable that equals one if the firm involved in the breach is a restaurant and zero if it is a hotel.
5. This is a two-tailed t-test of the hypothesis that the slope coefficient is not equal to zero. P-values give the level of confidence for the t-test.

return represents approximately a $2.7 billion loss in the value of these publicly traded hotel and restaurant firms. Second, we find that individual breach characteristics do not help predict the individual firm effect. That is, malicious events and repeat events are no better, nor worse, than other events. Third, the average hospitality firm faces no more value risk from a breach than a comparably sized retail firm. However, restaurants appear to be less impacted by data breaches than hotel firms. Thus, managers of hotel firms should raise their level of concern about potential data breaches because their firms appear to face greater value at risk from data breaches than restaurant firms. Managers of hospitality firms should be aware that predicting actualized breach costs based on firm specific data is difficult. This is seen in the lack of significance in some of the cross-sectional analysis. Finally, managers should not become complacent after a breach has occurred because subsequent breaches appear to be just as costly as first-time breaches.

Table 6. Test of Paired Sample with Off-Sample

t-Test: Two-Sample Assuming Unequal Variances

	(-1,+1) CAAR Sample	(-1,+1) CAAR Off-Sample
Mean	−0.012444753	−0.00392757
Variance	0.002418427	0.000459998
Observations	24	24
Hypothesized Mean Difference	0	
df	31	
t-Stat	−0.777721579	
P(T<=t) one-tail	0.221314242	
P(T<=t) two-tail	0.442628484	
Z Value	−0.2571	
P(T<=t) one-tail	0.3743	
P(T<=t) two-tail	0.79486	
Wilcoxon Test Matched Pair		
W Value	141	
N	24	
	Insignificant at 10%	

This paper is a first attempt to examine the impact of data breaches on hospitality firms. The sample size, at 24 data breaches, is relatively small compared to many other event studies. Hence it is not surprising that our summary and conclusions are somewhat tentative based upon a p-value of 6% for the overall CAAR. This leads us to three recommendations for future research. One, when more data breach observations for the hospitality industry become available the event study analysis should be re-run to verify the preliminary results provided in this paper. Two, a survey of IT managers would provide a means of understanding the different costs of data breaches. Finally, since the results provided in this paper represent the market's expectation of value effects, a study that examined post-breach firm performance may provide insights into the actualized costs of data breaches.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Proceeedings from: Workshop on the Economics of Information Security.* Robinson College, University of Cambridge, England.

Binder, J., & Summer, J. (1985). Measuring the effects of regulation with stock price data. *Rand Journal of Economics, 16*(2), 167–183.

Bloom, B. (2011). *Applications of event study methodology to lodging stock performance* (Doctoral dissertation). Retrieved from Theses and Dissertation Papers, Iowa State University. (11930).

Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of Financial Economics, 8*(3), 205–258.

Brown, S. J., & Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics, 14*(1), 3–31.

Campbell, K., Lawrence, G., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11,* 431–448.

Canina, L. (1996). Initial public offerings in the hospitality industry—Underpricing and overperformance. *Cornell Hospitality Quarterly, 37*(5), 18–26.

Canina, L. (2001). Acquisitions in the lodging industry: Good news for buyers and sellers. *Cornell Hospitality Quarterly, 42*(6), 47–54.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69–104.

Chang, C., & Zeng, Y. T. (2011). Impact of terrorism on hospitality stocks and the role of investor sentiment. *Cornell Hospitality Quarterly, 52*(2), 165–175.

Davies, R., & Kim, S. (2007). Using matched samples to test for differences in trade execution costs. *Babson Faculty Research Fund Working Papers.* Paper 4.

Garg, A., Curtis, J., & Harper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security, 11*(2/3), 74–83.

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

Hospitality Technology. (2017). Hotels unprepared when it comes to payment security. Retrieved from https://hospitalitytech.com/hotels-unprepared-when-it-comes-payment-security.

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

Hughes, J. S., Magat, W. A., & Ricks, W. E. (1986). The economic consequences of the OSHA dust standards: An analysis of stock price behaviour. *Journal of Law and Economics, 29*(1), 29–59.

Jarrell, G., & Peltzman, S. (1985). The impact of product recalls on the wealth of sellers. *Journal of Political Economics, 93*(3), 512–536.

Johnson, M., & Johnson, M. (2016). Federal tax law trumps Indian canon: Implications for the gaming industry. *Cornell Hospitality Quarterly, 57*(4), 434–441.

Johnson, M., Kang, M., & Lawson, T. (2017). Stock price reaction to data breaches. *Journal of Finance Issues, 16*(2), 1–13.

Johnson, M., Singh, A. J., & Ma, Q. (2015). The impact of authorization of the travel promotion act on hotel firm stock returns. *Cornell Hospitality Quarterly, 56*(1), 29–40.

Johnson, M., Singh, A. J., & Zhou, Y. (2015). Internet gaming: Valuation concerns for the industry. *Journal of Hospitality Financial Management, 23*(1), 25–44.

Kannan, K., Rees, J., & Sridhar, S. (2011). Market reactions to security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69–91.

Ma, Q., Zhang, W., & Chowdry, N. (2011). Stock performance of firms acquiring listed and unlisted lodging assets. *Cornell Hospitality Quarterly, 52*(3), 291–301.

Ponemon Institute. (2015). *Cost of data breach: Global overview.* Retrieved from https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

Privacy Rights Clearinghouse. (2014). Chronology of data breaches. Retrieved from https://www.privacyrights.org/data-breach/new.

SpiderLabs. (2015). *Trustwave global security report.* Retrieved from https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf.

Wyndham Worldwide Corporation. (2014). Press releases. Retrieved from http://www.wyndhamworldwide.com/news-media/wyndham-vacation-ownership-applauds-new-legislation-protecting-timeshare-owners.