DOI: 10.1111/risa.14122

ORIGINAL ARTICLE

Are the good spared? Corporate social responsibility as insurance against cyber security incidents

Vassiliki Bamiatzi[1] | Michael Dowling[2] | Fabian Gogolin[3] | Fearghal Kearney[4] | Samuel Vigne[5]

[1] University of Sussex Business School, University of Sussex, Brighton, UK

[2] Dublin City University Business School, Dublin City University, Dublin, Ireland

[3] Leeds University Business School, University of Leeds, Leeds, UK

[4] Queen's Management School, Queen's University Belfast, Belfast, UK

[5] Luiss Business School, Rome, Italy

Correspondence
Fearghal Kearney, Queen's Management School, Queen's University Belfast, 185 Riddel Hall, Stranmillis Road, Belfast BT9 5EE, UK.
Email: F.kearney@qub.ac.uk

Funding information
Irish Industrial Development Authority; Enterprise Ireland

Abstract

Despite the increasing consensus that socially responsible behavior can act as insurance against externally induced shocks, supporting evidence remains somewhat inconsistent. Our study provides a clear demonstration of the insurance-like properties of corporate social responsibility (CSR) in preserving corporate financial performance (CFP), in the event of a data (cyber) breach. Exploring a sample of 230 breached firms, we find that data breaches lead to significantly negative CFP outcomes for low CSR firms, with the dynamic being particularly pronounced in consumer-sensitive industries. Further, we show that firms increase their CSR activities in the aftermath of a breach to recover lost goodwill and regain stakeholder trust. Overall, our results support the use of CSR as a strategic risk-mitigation tool that can curtail the consequences of data breaches, particularly for firms operating in consumer-centric environments.

KEYWORDS
crisis management, cyber risk, insurance hypothesis, risk perception

1 | INTRODUCTION

With the relationship between corporate social responsibility (CSR) and corporate financial performance (CFP) remaining tenuous (Busch & Schnippering, 2022; Velte, 2021), research is increasingly tuned into the insurance properties of CSR in preserving, rather than generating financial performance (Godfrey et al., 2009; Minor & Morgan, 2011; Shiu & Yang, 2017). Indeed, more and more scholars now agree that socially responsible behavior can generate moral capital and goodwill, thereby creating an insurance-like mechanism (Barnett et al., 2018; Luo et al., 2018; Shiu & Yang, 2017).[1] For instance, Chen et al. (2022) use value-at-risk and lower partial moment measures to demonstrate that excellent CSR performance can alleviate downside risks. This mechanism can protect firms from negative events and offer better control of stakeholder expectations in crisis situations (Lins et al., 2017). However, the empirical evidence in support of the insurance hypothesis remains somewhat inconsistent (Awaysheh et al., 2020), with studies reporting contrasting findings even when examining the same type of events (Peloza, 2006). For example, studies looking at the consequences of oil spills have observed both positive (Luo et al., 2018) and negative (Luo et al., 2013) associations with CSR, indicating that CSR activities, depending on the event and its magnitude, can be both a benefit and a liability.[2]

Several meta-analytic studies have been put forward to shed light on the tenuous nature of the CSR–CFP relationship. While there is controversy over measurement issues

[1] Examples of other insurance-like mechanisms in related contexts include Klein and Dawar (2004) who report that CSR practices mitigate public outcry against firm liability in a product crisis, while Godfrey et al. (2009) show that firms known for their philanthropic activities observe a lower reputational backlash from any legal or regulatory violations. A good CSR strategy can also alleviate the negative implications of financial crises by enhancing profitability, stock price, and sales per employee (Lins et al., 2017; Schnietz & Epstein, 2005). More recently, Li et al. (2019) focus on China in establishing that CSR provides an insurance-like mechanism in protecting a firm against the reputational damage of being involved in tax avoidance, with Hadani et al. (2019) finding that corporate political activity limits the fallout of not complying with shareholder activism efforts.

[2] Luo et al. (2018) find that CSR activity, namely corporate philanthropy, is able to "ameliorate the negative consequences of oil spills." However, Luo et al. (2013) find that greener firms are more likely to have their accidents reported by the media and that the reporting is no less critical than at firms without a strong CSR record.

and sample variability, a consensus seems to be emerging toward a positive directionality between CSR and corporate performance. However, the relationship is highly contingent on different factors and moderators. For example, Friede et al. (2015) consider more than 2000 studies on the relationship between environmental, social, and governance criteria and CFP, and reveal that the vast majority find a non-negative and/or positive relationship. The relationship is strong across various regions, with North America and developed European countries showing the strongest associations. Wang et al. (2016) find that while the overall effect size of the CSR–CFP relationship is positive and significant, they highlight its tenuous nature by showing that CSR and CFP measurement strategies explain some of the variations observed. They uncover that the institutional environment a firm operates within is significant to the strength of the relationship and that the relationship is stronger for firms from advanced versus developing economies. Velte (2021), employing a qualitative meta-analysis, confirms that while both CSR and environmental performance increase CFP, the context of analysis plays an important role in the strength of the relationship. Finally, Busch and Schnippering (2022) specifically focus on the role of innovation, motivated by the ambiguous findings of how R&D intensity influences the corporate social performance (CSP)–CFP relationship. They find that extreme R&D intensity values contribute to elevated CFP and that overly simplistic functional misspecification of the innovation dynamic may have driven the inconclusive results in previous studies.

It is clear from the above discussion that the CSR–CFP relationship is conditional upon the context being explored—the region, the country, the industry, or even the timeframe. In this study, therefore, we take a context-specific view of the CSR–CFP relationship to observe the relationship under conditions of crisis. Despite acknowledging the role of CSR in protecting and preserving financial performance, to date, there is a paucity of literature on the ethics in risk decision-making under crisis conditions (Doorn, 2015). Utilizing the insurance and crisis management literature, we address this gap in the literature by looking at a very specific type of crisis: data breaches, a new type of event not previously investigated from a CSR–CFP perspective.

A data breach can be defined as a "*compromise of security that leads to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed*" (Knight & Nurse, 2020).[3] Therefore, such incidents may consist of different types of events, such as malware, ransomware, denial-of-service attacks, card payment fraud, malicious insiders, or even human error. Most data breaches can be attributed to external parties such as criminals, competitors, and hackers (including activist hackers, referred to, by some, as *hacktivists*). The average cost of a data breach in an enterprise or large organization has now reached $4.35 million (Ponemon Institute, 2022). Prominent examples include when Marriott International announced in 2018 that cyber thieves had stolen data on approximately 500 million customers. Even companies that are supposed to be at the front line of technological innovation and data protection, that is, Google, Yahoo, eBay, and Equifax, have been the subject of cyberattacks.[4] With the prevalence of cyberattacks increasing, posing threats at organizational (Paté-Cornell et al., 2018) and federal (Zheng & Albert, 2019) levels, studying data breaches with respect to the insurance capabilities of CSR can offer invaluable insights toward advancing our understanding of the CSR–CFP preservation relationship.

Meanwhile, in better examining the context-specific nature of the CSR–CFP relationship, we further focus on the industry-specific dimension of the CSR–CFP relationship. This study specifically considers firms with a strong consumer focus, on the premise that data breaches will challenge the trust and reputational foundation of consumer-focused businesses. Our study offers a number of distinct contributions to the literature. First, we explore the CSR–CFP relationship in relation to data breaches. We show that although data breaches have significant negative performance implications, a firm's CSR investment can provide insurance-like protection. We advance the existing theory on CSR as insurance by showing that this mechanism is particularly observable for firms operating in consumer-sensitive industries. Second, we add to the empirical literature on the insurance-like properties of CSR by exploring the ex-post implications of CSR in the aftermath of a data breach. This has become more pertinent when we consider that despite the increased risk of a company becoming a data breach victim (Ponemon Institute, 2022), many corporate executives believe their companies are unequipped to handle the fallout from a breach. Our findings denote that insurance properties of CSR can hence help alleviate stakeholder concerns over inadequate internal controls.

The study is structured as follows. We begin the next section by providing the key theoretical underpinnings that form the basis for our hypotheses. Next, we present our methodological framework, the empirical design, and data employed. We then present our findings and conclude with a discussion of our contribution to theory and practice.

2 | THEORETICAL BACKGROUND AND HYPOTHESES DEVELOPMENT

Business risks are inevitable in today's dynamic work environment (Baghersad & Zobel, 2022; Hashemi et al., 2019), with Christensen and Kohls (2003) identifying that crisis conditions are more likely as technology advances, meaning that recognizing and anticipating business risks is imperative for future success. Meanwhile, previous literature has highlighted a selection of benefits of incorporating ethical

[3] Cains et al. (2022) further standardize cyber security risk terminology in an interdisciplinary context.

[4] CSO. The 15 biggest data breaches of the 21st century (www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html).

considerations into risk analysis frameworks (Hansson & Aven, 2014; Rozell, 2018). More specifically, a good CSR strategy can act as a buffer against unexpected negative events and/or fraudulent actions that could affect a firm's reputation and performance. Therefore, this growth in business risk increases the need to understand the "insurance mechanism hypothesis" dimension of CSR strategies (Godfrey et al., 2009; Koh et al., 2014; Minor & Morgan, 2011; Shiu & Yang, 2017)

During times of crisis, companies are often accused of ignoring their most important stakeholders (Sellnow et al., 2012). However, it can be argued that companies that introduce CSR activities enjoy higher levels of trust and understanding from their stakeholders. In these cases, a firm's stakeholders may exhibit higher resilience in response to a negative incident (Cheng et al., 2014; Lins et al., 2017), especially when it is externally initiated, temporary, and uncontrollable, as stakeholders are more likely to accept an incident as "an honest mistake" or simply bad luck, rather than as bad management and negligence (Klein & Dawar, 2004; Minor & Morgan, 2011). Meanwhile, a firm showcasing sensitivity to social and moral concerns is expected to portray the same behavior toward its external and internal actors. In other words, employees that perceive their firm as "doing good" may be discouraged from rouge or outright illegal activities, therefore reducing the internal threat of a breach (Koh et al., 2014). Campbell (2007) and Li et al. (2019) also highlight the importance of employees, by identifying the presence of employee associations, as well as state regulation and nongovernmental organizations (NGOs), as factors leading to firms being more likely to engage in a socially responsible manner. Doh and Guay (2006) demonstrate the role of advocacy by NGOs in encouraging such responsible behavior by firms. More directly, Sen and Borle (2015) highlight how stricter laws reduce the risk of data breaches, which aligns with Velte (2021) who presents the benefits of increased government regulation in the form of stronger CSR reporting requirements.

Taking the above into consideration, we expect that higher CSR activities lessen the negative implications of a cyber breach, act as a shield against public opinion and outcry, and preserve corporate reputation. Therefore, we posit that:

Hypothesis 1. *Higher CSR activity lessens the effects of data breaches on firm performance.*

Consumer reactions differ greatly across shocks and industries (Figuié & Fournier, 2008; Wei et al., 2016). Data breaches are one such shock that impacts consumers directly, with Ponemon Institute (2022) citing that 60% of firms are raising prices due to the impact of data breaches. Yet, the implications of data breaches for consumer sentiment have only briefly been explored in the literature. Some examples include Das et al. (2012) and Tosun (2021), with Das et al. (2012) reporting that depending on the type of attack, web-based (i.e., e-commerce firms) and banking, financial services, and insurance companies suffer more severely from cyberattacks. Eling and Jung (2018) also find that data loss severity is highest for retail/merchant and banking and insurance industry sectors. The service provision of these companies depends heavily on the internet and as a result, they handle large volumes of confidential information such as customer PINs, social security numbers, and credit card data (Das et al., 2012).

Motivated by the above, we expect the impact of a data breach to be more severe for firms operating in high consumer-sensitive industries, that is, firms that produce goods and services primarily aimed at individual customers (Lev et al., 2010), for example, retail, food, and beverage. This is in contrast to low consumer-sensitive industries that primarily produce goods and services to meet industrial or governmental demand, for example, commercial aircraft manufacturers. Our expectations are based on two key premises. First, in high consumer-sensitive industries, consumers will be more attuned to the use, protection, and dissemination of their personal information, since any mishandling can have detrimental effects on their personal and professional lives. Recent reports on the pervasiveness of data breaches, for example, IBM's Cost of a Data Breach Report (Ponemon Institute, 2022), suggest that customers are becoming more sensitive and demanding when it comes to the handling of their personal data. Second, we expect that firms operating in industries that either handle large quantities of sensitive data or rely on consumer data (such as companies operating in high consumer-sensitive industries) to be "lucrative targets for financially-motivated cyber attackers" (Das et al., 2012). As Lev et al. (2010) succinctly put it: "firms that produce goods and services for individual customers (high consumer sensitivity) have greater incentive to appear charitable…than firms that produce goods and services for industrial or government use (low consumer sensitivity)".

While there is ample evidence suggesting that CSR practices differ substantially across firms (Chen et al., 2022), and the position of a firm in the value chain (Kim et al., 2019), our understanding of the context-specific nature of CSR-CFP remains fragmented, unbalanced, and incomplete (Dabic et al., 2016). As CSR can significantly influence consumer attitudes, purchase intentions, loyalty, satisfaction, and consequently their evaluation of a company and its products, we argue that the negative impact of a security breach will be exacerbated within a consumer-sensitive industry but significantly alleviated by increased CSR engagement.

Hypothesis 2a. *Firms in high consumer-sensitive industries will experience lower firm performance due to data breaches, compared to those in low consumer-sensitive industries.*

Hypothesis 2b. *In high consumer-sensitive industries, higher CSR activity will lessen the negative effects of data breaches on firm performance at a greater level than in low consumer-sensitive industries.*

On the other hand, we recognize that during times of crises there are different strategies that a firm can employ including apologizing, remuneration as well as price reductions and additional advertising (Löfstedt & Renn, 1997; Pfarrer et al., 2008). While these tactics are important, they do little to repair damaged stakeholder relationships and hence are insufficient in recovering stakeholder trust. On the contrary, we expect that explicit social acts can help firms to more efficiently rehabilitate their public image (Pfarrer et al., 2008). As mentioned for H1, increased CSR activities, targeting the general public and/or the affected stakeholders will increase stakeholders' conviction that such an incident was indeed a "one-time occurrence" (Klein & Dawar, 2004; Minor & Morgan, 2011), and reinforce their trust against a future recurrence. Such an approach not only increases the integrity and courage to cope with the aftermath of a crisis (Shrivastava, 1993) but also strengthens the legitimacy and fairness of the decisions made.

Ulmer and Sellnow (2000) theorized that a crisis often leads to greater protection of internal stakeholders at the expense of external stakeholders. However, several experimental studies find that CSR can appease a multitude of stakeholders during a post-crisis period (Assiouras et al., 2013; Vassilikopoulou et al., 2009). In this way, CSR serves as an asset to expedite a firm's recovery from reputational damage suffered as a result of a crisis. Finally, the more reliant a firm's business model is on a particular group of stakeholders, the greater the need to address stakeholders effectively post-crisis. Therefore, we posit that:

Hypothesis 3. *Firms in high consumer-sensitive industries will take actions to enhance CSR performance to a greater degree in the aftermath of data breaches, in comparison with firms in low consumer-sensitive industries.*

3 | DATA AND METHODOLOGY

3.1 | CSR data

In this study, we combine several data sets. First, to measure CSR activities, we employ the KLD Stats database constructed by KLD Research. The KLD database assesses a firm's corporate social performance within seven dimensions: community, diversity, employee relations, environment, human rights, product, and corporate governance. Each of these dimensions includes several strength and concern subcategories that are rated either 0 (neutral) or 1 (strength/concern). We construct a CSR measure based on the first six categories (community, diversity, employee relations, environment, human rights, and product). Corporate governance is excluded from our primary measure as it is not directly related to a firm's CSR activities (Jian & Lee, 2015; Servaes & Tamayo, 2013); however, we later check for robustness to including corporate governance in the CSR score calculation in the acknowledgement of the recent growth in the popularity of the "ESG" movement. For each firm-year observation, we aggregate all strengths and concerns across the six dimensions and calculate the annual measure by subtracting a firm's total CSR concerns from its total CSR strengths. To test our hypothesis, we use the net CSR measure (and lagged values of this score) as our CSR measure. We supplement our calculated CSR scores with accounting data from Compustat and stock market data from CRSP. We follow Servaes and Tamayo (2013) by matching the concurrent CSR score to firms with a December fiscal year-end. For firms with a fiscal year-end prior to December, we match the KLD data from the previous year to make sure that CSR scores precede performance measures and firm-level controls.

To define consumer-sensitive firms, that produce goods and services primarily aimed at individual customers (Lev et al., 2010), we use Compustat SIC codes: 0000–0999, 2000–2399, 2500–2599, 2700–2799, 2830–2869, 3000–3219, 3420–3429, 3523, 3600–3669, 3700–3719, 3751, 3850–3879, 3880–3999, 4813, 4830–4899, 5000–5079, 5090–5099, 5130-5159, 5220–5999, 7000–7299, and 7400–9999.

3.2 | Data breaches

To identify data breaches, we use the Privacy Rights Clearinghouse (PRC) database. PRC is a California-based nonprofit corporation that collects detailed information about cyber security breaches for businesses, nonprofits organizations, and government organizations in the United States. Each recorded breach is verified through media sources or government agencies. The adoption of Security Breach Notification Laws across the United States as well as increased media attention has driven the use of PRC data in empirical research (Eling & Jung, 2018; Higgs et al., 2016).

Examples of breaches classified by the PRC include incidents due to credit/debit card fraud; hacks by malware or a malicious outside party; malicious insiders; lost, discarded, or stolen physical devices, documents, laptops, smartphones, memory sticks, and hard-drives; and unintended disclosures of sensitive information. We restrict our sample to incidents that affect publicly traded firms. Finally, to avoid the influence of previous incidents, we include only the first cyber security breach for each firm in our sample. Using the PRC database, we identify 230 firms breached within the KLD database.

3.3 | Variables

Our main performance measure is profitability, calculated as return on assets (ROA). This measure has been widely used to assess performance in relation to a firm's CSR activities (Jo & Harjoto, 2012; Petrenko et al., 2016; Servaes & Tamayo, 2013). Following Petrenko et al. (2016), we calculate ROA as net income divided by total assets. For robustness, we further calculate return on equity (ROE) and return on sales (ROS) (Jian & Lee, 2015; Servaes & Tamayo, 2013) to represent alternative short-term indicators, and Tobin's Q as a longer term profitability measure (Lenz et al., 2017; Mishra, 2017).

Size and market value are especially important control variables in relation to data breaches. Both large and valuable firms have greater visibility and attract more media attention. As a result, they are more likely to become targets for potential adversaries (Kamiya et al., 2021). We use the logarithms of size and market-to-book ratio to control for size and visibility effects (Kamiya et al., 2021). Acknowledging that firms producing highly specialized products and those in possession of trade secrets are more likely to be targeted by cyberattacks (Ettredge et al., 2018), we control for firm-level R&D expenses, and intangibles measured as 30% of selling, general and administrative expenses plus R&D expenses as per Peters and Taylor (2017). Stock return and risk control variables are calculated using daily stock returns and standard deviations for the firm's fiscal year. We further include an indicator variable equal to 1 if a firm pays a dividend. Finally, leverage is calculated as a firm's current liabilities plus long-term debt divided by total assets. Our final sample includes 5092 firm-year observations for 638 firms. Definitions of the variables used in our study are given in Table A1.

3.4 | Methodology

3.4.1 | Data breaches and CSR

In the first step of our analysis, in line with the first hypothesis (H1), we test the insurance-like capabilities of CSR in relation to data breaches. We estimate the following model:

$$\begin{aligned}&\mathit{Profitability}_{i,t} = \alpha + \beta \mathit{Data\_breach}_{i,t-1} + \beta \mathit{CSR\_score}_{i,t-1}\\&+\beta \mathit{Data\_breach}_{i,t-1} \times \mathit{CSR\_score}_{i,t-1} + \gamma X + \delta + \lambda + \mu_{i,t}.\end{aligned} \tag{1}$$

Our outcome variable $\mathit{Profitability}_{i,t}$ is defined as a firm's return on assets at time t for firm i. $\mathit{Data\_breach}_{i,t-1}$ is a dummy variable equal to 1 if a firm suffered a data breach in year $t-1$ and $\mathit{CSR\_score}_{i,t-1}$ is a firm's CSR score at time $t-1$. All right-hand-side variables are lagged by one period to account for the fact that we employ balance sheet data throughout our analysis. The variable of interest is the interaction term $\mathit{Data\_breach}_{i,t-1} \times \mathit{CSR\_score}_{i,t-1}$. The interaction term captures the effect of a data breach in relation to a firm's CSR score. To control for important firm characteristics, known to impact a firm's profitability, we further include a vector of time-varying control variables (X), as well as vectors of industry (δ) and time (λ) dummies.

3.4.2 | Data breaches, CSR, and consumer-sensitive industries

In the second step of our analysis, we are interested in the importance of consumer sensitivity in relation to the ability of CSR to serve as an insurance-like mechanism. We follow Lev et al. (2010) and define consumer-sensitive industries as those that fall into either of the two classifications, consumer goods or finance.[5]

Roughly 67% of the 638 firms in our sample are classified as consumer-sensitive. Panel C of Table 1 further outlines that 3423 (153) firm-year observations (data breaches) are classified as consumer-sensitive with 1669 (77) firm-year observations (data breaches) deemed to be non-consumer-sensitive industries. We re-estimate Equation 1 to include an indicator variable, $\mathit{Consumer\text{-}sensitive\_industry}_i$, that is equal to 1 if a firm operates in a consumer-sensitive industry, and 0 otherwise:

$$\begin{aligned}&\mathit{Profitability}_{i,t} = \alpha + \beta \mathit{Data\_breach}_{i,t-1} + \beta \mathit{CSR\_score}_{i,t-1}\\&+\beta \mathit{Consumer} - \mathit{sensitive\_industry}_i + \beta \mathit{Data\_breach}_{i,t-1}\\&\times \mathit{CSR\_score}_{i,t-1} + \beta \mathit{Data\_breach}_{i,t-1} \times \mathit{CSR\_score}_{i,t-1}\\&\times \mathit{Consumer} - \mathit{sensitive\_industry}_i + \gamma X + \delta + \lambda + \mu_{i,t}.\end{aligned} \tag{2}$$

The variable of interest in this second model is the following interaction term: $\mathit{Data\_breach}_{i,t-1} \times \mathit{CSR\_score}_{i,t-1} \times \mathit{Consumer\text{-}sensitive\_industry}_i$. This interaction term captures the insurance-like capabilities of CSR in relation to data breaches for firms operating in consumer-sensitive industries. As we did in Equation 1, we control for important firm characteristics, known to impact a firm's profitability (X), as well as vectors of industry (δ) and time dummies (λ).

3.4.3 | Post-breach CSR and consumer-sensitive industries

Finally, we examine how firms adjust their CSR activities in the aftermath of a breach, with a particular focus on firms that operate in a consumer-sensitive business environment. Our outcome variable, $\mathit{CSR\_score}_{i,t}$, is the CSR score for firm i at time t. To capture the contemporaneous and subsequent impacts of a data breach, we include three different versions of the indicator variables *Data_breach/Post_breach*. First, to capture the contemporaneous impact of the breach, we estimate the following regression model, where $\mathit{Data\_breach}_{i,t}$ is equal 1 if the firm experienced a breach in that year:

$$\begin{aligned}&\mathit{CSR\_score}_{i,t} = \alpha + \beta \mathit{Data\_breach}_{i,t} + \beta \mathit{Consumer}\\&- \mathit{sensitive\_industry}_i + \beta \mathit{Data\_breach}_{i,t} \times \mathit{Consumer}\\&- \mathit{sensitive\_industry}_i + \gamma X + \delta + \lambda + \mu_{i,t}.\end{aligned} \tag{3}$$

The variable of interest here is the interaction term $\mathit{Data\_breach}_{i,t} \times \mathit{Consumer\text{-}sensitive\_industry}_i$.

Second, we focus on the impact of the breach one period after it has occurred, where $\mathit{Post\_breach}_{i,t+1}$ is equal to 1 if

[5] We define consumer-sensitive companies as those with Compustat SIC codes: 0000–0999, 2000–2399, 2500–2599, 2700–2799, 2830–2869, 3000–3219, 3420–3429, 3523, 3600–3669, 3700–3719, 3751, 3850–3879, 3880–3999, 4813, 4830–4899, 5000–5079, 5090–5099, 5130–5159, 5220–5999, 7000–7299, 7400–9999. Finance companies are defined as those with SIC codes: 6000–6999.

TABLE 1 Sample distribution. This table reports the distribution of our sample across three dimensions. Panel A reports the distribution of observations and data breaches per year, Panel B provides an industry breakdown of the sample (Fama-French 12 Industry Classification), and Panel C shows the observations and data breaches for firms operating in consumer-sensitive industries

Panel A: Distribution by year		
Year	**Observations**	**Data breaches**
2005	490	11
2006	489	31
2007	493	29
2008	499	18
2009	525	11
2010	517	28
2011	521	26
2012	527	26
2013	515	27
2014	516	23
Total	5092	230
Panel B: Distribution by industry		
Industry	**Observations**	**Data breaches**
Consumer Non-durables	367	6
Consumer durables	95	4
Manufacturing	583	11
Oil, gas, and coal extraction	317	2
Chemicals and allied products	195	1
Business equipment	805	33
Telephone and television transmission	137	18
Utilities	348	6
Wholesale, retail, and some services	576	49
Healthcare, medical equipment, and drug	356	4
Finance	796	77
Other	517	19
Total	5092	230
Panel C: Distribution by consumer-sensitive industry		
Type of industry	**Observations**	**Data breaches**
Consumer-sensitive industry	3423	153
Non-consumer-sensitive industry	1669	77
Total	5092	230

the firm experienced a breach one year previously:

$$CSR\_score_{i,t} = \alpha + \beta Post\_breach_{i,t+1} + \beta Consumer - sensitive\_industry_i + \beta Post\_breach_{i,t+1} \times Consumer - sensitive\_industry_i + \gamma X + \delta + \lambda + \mu_{i,t}. \quad (4)$$

Again, the variable of interest here is the interaction term, in this case, $Post\_breach_{i,t+1}$ × *Consumer-sensitive_industry*$_i$.

Finally, we look at the impact of the breach in the t+1 to t+2 period, where $Post\_breach_{i,t+2}$ is equal to 1 if the firm experienced a breach 1–2 years previously:

$$CSR\_score_{i,t} = \alpha + \beta Post\_breach_{i,t+2} + \beta Consumer - sensitive\_industry_i + \beta Post\_breach_{i,t+2} \times Consumer - sensitive\_industry_i + \gamma X + \delta + \lambda + \mu_{i,t}. \quad (5)$$

Again, the variable of interest here is the interaction term, in this case, $Post\_breach_{i,t+2}$ × *Consumer-sensitive_industry*$_i$.

As per previous specifications, we include an indicator variable that is equal to 1 if a firm operates in a consumer-sensitive industry, *Consumer-sensitive_industry*$_i$, and zero otherwise. We also control for firm-level differences as well as differences across industries (δ) and time (λ).

4 | RESULTS

4.1 | Distribution, summary statistics, and correlation analysis

The distribution of data breaches in our sample is given in Table 1. Panel A presents the distribution across years, Panel B presents the distribution across industries (Fama-French 12 Industry Classification), and finally, in Panel C we provide a breakdown by a consumer-sensitive industry. Table 2 presents summary statistics for all the main variables. Finally, a correlation matrix is provided in Table 3. Our final sample includes 5092 observations across 638 firms with 230 identified data breaches. The data breaches are relatively equally dispersed throughout the sample period. In terms of distribution across industries, the concentration is highest for companies operating in telephone and television transmission. Overall, we find that approximately 4% of firms in our sample have suffered a data breach with the majority of them, roughly 67%, classified as operating in consumer-sensitive industries. Furthermore, the correlation analysis reveals that total assets as an indicator of firm size and visibility are most strongly correlated (0.313) with a firm suffering a breach.

4.2 | CSR as insurance: The case of data breaches

In the first part of our empirical analysis, we test the insurance-like characteristics of a firm's CSR activities in relation to data breaches. The insurance argument predicts that CSR can protect firms from negative consequences after an event or shock. We apply the same rationale to data breaches and evaluate their impact on firm financial performance.

TABLE 2 Summary statistics. This table reports summary statistics. In particular, the table reports the number of observations for all the variables used throughout our regression analysis. Furthermore, the table reports the mean and median value of each variable, its standard deviation as well as the 10th (P10) and 90th (P90) percentile of the distribution

Summary statistics	Observations	Mean	Median	Standard deviation	P 10	P 90
CSR_score	5092	1.542	1.000	3.546	−2.000	6.000
CSR_score(Gov)	5092	1.128	1.000	3.834	−3.000	6.000
Consumer-sensitive_industry	5092	0.672	1.000	0.469	0.000	1.000
Data_breach	5092	0.045	0.000	0.208	0.000	0.000
ROA	5092	0.058	0.065	0.085	0.001	0.139
ROE	5092	0.012	0.055	0.567	0.006	0.100
ROS	5092	0.087	0.083	0.268	0.005	0.215
Tobins_Q	5092	1.897	1.559	1.129	1.000	3.177
R&D	5092	0.021	0.000	0.043	0.000	0.076
Intangibles	5092	0.071	0.051	0.076	0.000	0.173
Size	5092	49,062	10,910	180,939	2,345	79,939
Market-to-book	5092	1.489	1.188	1.181	0.440	2.859
Stock_return	5092	0.075	0.047	0.492	−0.332	0.425
Risk	5092	68.131	47.590	47.589	10.354	162.181
Dividend	5092	0.763	1.000	0.430	0.000	1.000
Leverage	5092	0.243	0.224	0.172	0.033	0.464

Abbreviations: ROA, return on assets; ROE, return on equity.

Table 4 presents OLS regression results based on Equation 1 for a number of lagged firm variables on our outcome variable, ROA. We employ a variety of specifications. First, in columns (1), (3), and (5), we capture the knowledge-based investment of a firm using a firm's R&D expenditure. Second, in columns (2), (4), and (6), we include a measure of intangibles to also capture some of the innate organizational capital of a firm (Lev & Radhakrishnan, 2005). We also control for year effects in columns (1) and (2) and year and industry effects in columns (3–6). As corporate governance may also be included in decisions made by investors regarding CSR, columns (5) and (6) adopt an alternative calculation for the CSR score that includes the corporate governance category.

In line with our expectations, we find that data breaches have a negative impact on firm profitability. The negative effect ranges from 0.9% to 2.5% across our regression specifications. While, as in prior studies, we find an insignificant coefficient for the CSR variable capturing the direct relationship between CSR and performance, we do reveal an indirect relationship. We find that the interaction term is significant and positive across all specifications, indicating that CSR (calculated with or without the corporate governance dimension) lessens the negative impact of a data breach, thus providing support for our first hypothesis (H1). Overall, our results support the view that CSR can shield firms against negative performance implications arising from data breaches. For robustness, we also consider alternative firm performance specifications, namely short-term (ROE and ROS) and long-term profitability measures (Tobin's *Q*). Table A2 presents the results of this analysis. Again, focusing on the key interaction term between a data breach and the CSR score, we find that these alternative profitability specifications also broadly support our first hypothesis (H1). Similar to Table 4, the widespread significance of the interaction term suggests that CSR can protect firms against the financial impact of data breaches.

4.3 | CSR as insurance: The case of data breaches in consumer-sensitive industries

While the empirical evidence of the insurance provision of CSR is growing (Koh et al., 2014; Shiu & Yang, 2017), the existing research predominantly focuses on the type of event and the way it may affect firms. So far, existing research has placed little emphasis on the stakeholder group most affected by the examined negative firm-specific event, the customers. While we acknowledge that firm heterogeneity within sectors can result in significant variation (Welburn & Strong, 2022), to address our second set of hypotheses, we concentrate on examining financial performance effects for breached firms operating in consumer-sensitive industries. Results are reported in columns (1–6) of Table 5. We include the same set of control variables as in Table 4. However, for the sake of brevity, we do not report each control variable individually. As in Table 4, we control for year effects in columns (1) and (2), and year and industry fixed-effects in columns (3–6).

TABLE 3 Correlation matrix. This table reports the correlation coefficients between the main variables used throughout this study. The reported coefficients are for the full sample (N = 5092)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1. CSR_score	1.000															
2. CSR_score(Gov)	0.977	1.000														
3. Data_breach	0.079	0.061	1.000													
4. ROA	0.070	0.074	−0.038	1.000												
5. ROE	0.029	0.040	0.006	0.335	1.000											
6. ROS	0.069	0.076	−0.021	0.393	0.536	1.000										
7. Tobins_Q	0.066	0.066	−0.030	0.522	0.046	0.138	1.000									
8. Consumer-sensitive_industry	−0.027	−0.018	−0.003	−0.139	0.008	0.028	−0.201	1.000								
9. R&D	0.221	0.192	−0.029	0.044	−0.007	0.009	0.293	0.005	1.000							
10. Intangibles	0.190	0.168	−0.031	0.193	0.006	−0.022	0.426	−0.332	0.741	1.000						
11. Total_assets	0.122	0.073	0.313	−0.110	−0.038	−0.035	−0.151	0.100	−0.090	−0.170	1.000					
12. Market-to-book	0.053	0.055	−0.045	0.558	0.053	0.145	0.989	−0.210	0.319	0.450	−0.179	1.000				
13. Stock_return	−0.004	−0.004	0.001	0.046	0.102	0.057	0.089	−0.002	0.002	−0.020	0.041	0.082	1.000			
14. Risk	−0.133	−0.130	−0.014	0.105	−0.035	0.029	0.171	0.105	−0.042	−0.135	0.023	0.158	0.001	1.000		
15. Dividend	0.061	0.086	0.036	0.030	0.046	0.032	−0.175	0.023	−0.319	−0.299	0.103	−0.210	−0.064	−0.003	1.000	
16. Leverage	−0.052	−0.049	−0.014	−0.200	−0.074	−0.040	−0.139	−0.125	−0.175	−0.222	0.036	−0.114	−0.013	−0.047	0.098	1.000

Abbreviations: ROA, return on assets; ROE, return on equity, ROS, return on sales.

TABLE 4 Data breaches, corporate social responsibility (CSR), and firm profitability. This table reports the results of a linear regression model with *Profitability* (return on assets, ROA) as the dependent variable. *Data_breach* is an indicator variable equal to 1 if the firm suffered a data breach and 0 otherwise. *CSR_score* is the firm's CSR score computed based on KLD data, with *CSR_score(Gov)* incorporating the corporate governance category when calculating the CSR measure. The variable of interest is the interaction term *Data_breach*×*CSR_score*

					CSR_score(Gov)	
	ROA					
	(1)	**(2)**	**(3)**		**(5)**	**(6)**
Data_breach$_{(t-1)}$	−0.025**	−0.025**	−0.024**	−0.024**	−0.011**	−0.009*
	(−2.34)	(−2.30)	(−2.17)	(−2.18)	(−2.10)	(−1.84)
CSR_score$_{(t-1)}$	0.000	0.000	0.001	0.001	0.001	0.001
	(0.65)	(0.39)	(1.15)	(1.05)	(1.63)	(1.64)
Data_breach$_{(t-1)}$ × *CSR_score*$_{(t-1)}$	0.003**	0.003**	0.003**	0.003**	0.003**	0.003**
	(2.05)	(2.04)	(2.00)	(2.02)	(2.12)	(2.13)
R&D$_{(t-1)}$	−0.109*		−0.043		−0.503*	
	(−1.93)		(−0.79)		(−1.89)	
Intangibles $_{(t\ -1)}$		−0.028		−0.001		−0.241*
		(−0.94)		(−0.03)		(−1.96)
Log(*Size*$_{(t-1)}$)	0.003	0.003	0.003	0.003	0.005**	0.003
	(1.60)	(1.37)	(1.54)	(1.54)	(2.46)	(1.63)
Log(*Market-to-book*$_{(t-1)}$)	0.083***	0.082***	0.085***	0.084***	0.059***	0.059***
	(18.84)	(18.05)	(18.01)	(17.66)	(16.04)	(15.81)
Stock_return$_{(t-1)}$	0.011***	0.011***	0.010***	0.011***	0.002**	0.002**
	(2.72)	(2.74)	(2.67)	(2.69)	(2.07)	(2.03)
Risk$_{(t-1)}$	−0.000	−0.000	−0.000	−0.000	0.000	0.000
	(−1.10)	(−1.19)	(−1.06)	(−1.05)	(1.36)	(1.31)
Dividend $_{(t\ -1)}$	0.013***	0.015***	0.009*	0.009*	0.013***	0.014***
	(3.13)	(3.57)	(1.87)	(1.94)	(3.16)	(3.50)
Leverage $_{(t\ -1)}$	−0.021*	−0.019*	−0.025**	−0.024**	−0.143***	−0.147***
	(−1.89)	(−1.75)	(−2.09)	(−2.01)	(−3.14)	(−3.96)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes	Yes	Yes
Observations	5092	5092	5092	5092	5092	5092
R^2	0.117	0.118	0.133	0.134	0.177	0.165

Note: All explanatory variables are lagged by one time period. *t*-Statistics given in parentheses are based on standard errors corrected for heteroskedasticity and firm-level clustering. Asterisks ***, **, and * indicate statistical significance at 1%, 5%, and 10% levels, respectively.

First, we observe that the negative impact of data breaches on firm profitability is centered around firms operating in consumer-sensitive industries (H2a). This is an important finding as it provides the first explicit evidence to link the negative consequences of an event (in this case data breaches) to the reaction of a particular stakeholder group. Most importantly, however, we find that the insurance provision of CSR is also concentrated around firms that operate in a consumer-sensitive environment (H2b). In comparison with Table 4, the potential of CSR to provide insurance-type provisions in times of crisis is stronger once the consumer-sensitivity of the firm's business environment has been accounted for. Again, this result is robust to the inclusion of corporate governance in the CSR score calculation as shown in columns (5) and (6). In line with our previous results, we observe no significant relationship between CSR and firm performance, showing that the potential for CSR to impact performance is constrained to its insurance provision.

4.4 | Post-breach CSR in consumer-sensitive industries

In the final stage of our empirical analysis, we examine changes in CSR activities due to a data breach for consumer-sensitive firms. We expect that firms increase their CSR activity to repair stakeholder trust and positively alter stakeholder evaluations after a crisis. For this analysis our

TABLE 5 Data breaches, corporate social responsibility (CSR), and firm profitability in consumer-sensitive industries. This table reports the results of a linear regression model with *Profitability* (return on assets, ROA) as the dependent variable. *Data_breach* is an indicator variable equal to 1 if the firm suffered a data breach and 0 otherwise. *CSR_score* is the firm's CSR score computed based on KLD data, with *CSR_score(Gov)* incorporating the corporate governance dimension when calculating the CSR measure. We further define an indicator variable *Consumer-sensitive_industry* if a firm operates in a consumer-sensitive industry. The variable of interest is the interaction term *Data_breach*×*CSR_score*×*Consumer-sensitive_industry*

					CSR_score(Gov)	
	ROA					
	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
Data_breach$_{(t-1)}$	−0.008	−0.007	−0.006	−0.006	−0.006	−0.006
	(−0.70)	(−0.69)	(−0.56)	(−0.57)	(−0.50)	(−0.50)
CSR_score$_{(t-1)}$	−0.000	−0.000	−0.000	−0.000	0.000	0.000
	(−0.48)	(−0.62)	(−0.29)	(−0.34)	(0.85)	(0.73)
Data_breach$_{(t-1)}$ × *CSR_score*$_{(t-1)}$	0.000	0.000	0.000	0.000	−0.000	−0.000
	(0.25)	(0.26)	(0.27)	(0.29)	(−0.29)	(−0.24)
Consumer-sensitive_industry	0.001	−0.001	0.005	0.006	−0.000	0.002
	(0.20)	(−0.19)	(1.10)	(1.19)	(−0.04)	(0.27)
Data_breach$_{(t-1)}$ × *Consumer-sensitive_industry*	−0.034*	−0.034*	−0.033*	−0.033*	−0.015*	−0.016*
	(−1.87)	(−1.88)	(−1.87)	(−1.88)	(−1.85)	(−1.87)
CSR_score$_{(t-1)}$ × *Consumer-sensitive_industry*	−0.000	−0.000	0.000	0.000	−0.000	−0.000
	(−0.36)	(−0.50)	(0.13)	(0.07)	(−0.19)	(−0.22)
Data_breach$_{(t-1)}$ × *CSR_score*$_{(t-1)}$ × *Consumer-sensitive_industry*	0.005**	0.005**	0.005**	0.005**	0.004**	0.004**
	(2.05)	(2.04)	(2.00)	(1.98)	(1.96)	(2.02)
Control for R&D	Yes	No	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes	Yes	Yes
Observations	5092	5092	5092	5092	5092	5092
R^2	0.119	0.120	0.136	0.137	0.124	0.126

Note: All time-dependent explanatory variables are lagged by one time period. *t*-Statistics given in parentheses are based on standard errors corrected for heteroskedasticity and firm-level clustering. Asterisks ***, **, and * indicate statistical significance at 1%, 5%, and 10% levels, respectively.

dependent variable is now *CSR_score*. Again, we include two measures of innate organizational capital: (i) R&D and (ii) intangible assets (Lev & Radhakrishnan, 2005). We control for all previously employed firm-level control variables, as well as year and industry dummies. The results are presented in Table 6. We report three different specifications: (i) contemporaneous changes in CSR are reported in Panel A, (ii) changes in the year after the breach (t + 1) are reported in Panel B, and finally (iii) changes in 2 years after the breach (t + 1 to t + 2) are reported in Panel C.

We find evidence that firms operating in consumer-sensitive industries increase their CSR activities after a data breach. Based on the interaction term in each panel, there is no evidence that a firm will increase its CSR score in the year of the breach. Rather, we predominantly observe an increase in the CSR score in the year following the breach (H3). Our results imply that firms deal with the immediate consequences of a breach in the year it occurs (Panel A) but are able to shift focus towards appeasing stakeholders and regaining trust in subsequent years (Panels B and C). Moreover,

TABLE 6 Post-breach corporate social responsibility (CSR). This table reports the results of a linear regression model with *CSR_score* as the dependent variable. *Data_breach* is an indicator variable that is equal to one in the year of the data breach. *Post_breach* is an indicator variable that specifies two time periods after a firm suffered a data breach: (i) the year after the data breach, *Post_breach*$_{(t+1)}$, and (ii) the second year subsequent to the data breach, *Post_breach*$_{(t+2)}$

Panel A	***CSR_score***			
	(1)	**(2)**	**(3)**	**(4)**
Data_breach$_{(t)}$	0.112	0.101	0.088	0.086
	(0.41)	(0.36)	(0.31)	(0.30)
Consumer-sensitive_industry	−0.336*	−0.081	−0.790***	−0.707***
	(−1.78)	(−0.41)	(−2.89)	(−2.64)
Data_breach$_{(t)}$ × *Consumer-sensitive_industry*	−0.087	−0.097	−0.082	−0.090
	(−0.23)	(−0.25)	(−0.21)	(−0.23)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	4495	4495	4495	4495
R^2	0.283	0.283	0.285	0.284

Panel B	***CSR_score***			
	(1)	**(2)**	**(3)**	**(4)**
Post_breach$_{(t+1)}$	−0.166	−0.147	−0.168	−0.158
	(−0.49)	(−0.44)	(−0.50)	(−0.47)
Consumer-sensitive_industry	−0.366*	−0.109	−0.833***	−0.751***
	(−1.95)	(−0.55)	(−3.05)	(−2.80)
Post_breach$_{(t+1)}$ × *Consumer-sensitive_industry*	0.966**	0.922**	0.956**	0.936**
	(2.21)	(2.13)	(2.18)	(2.14)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	4495	4495	4495	4495
R^2	0.283	0.282	0.285	0.284

Panel C	***CSR_score***			
	(1)	**(2)**	**(3)**	**(4)**
Post_breach$_{(t+2)}$	0.081	0.097	0.084	0.095
	(0.22)	(0.27)	(0.23)	(0.26)
Consumer-sensitive_industry	−0.371**	−0.114	−0.844***	−0.762***
	(−1.98)	(−0.58)	(−3.09)	(−2.84)
Post_breach$_{(t+2)}$ × *Consumer-sensitive industry*	0.844*	0.806*	0.817*	0.799*
	(1.80)	(1.73)	(1.73)	(1.70)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes

(Continues)

TABLE 6 (Continued)

Panel C	*CSR_score*			
	(1)	**(2)**	**(3)**	**(4)**
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	4495	4495	4495	4495
R^2	0.284	0.283	0.286	0.285

Note: *t*-Statistics given in parentheses are based on standard errors corrected for heteroskedasticity and firm-level clustering. Asterisks ***, **, and * indicate statistical significance at 1%, 5%, and 10% levels, respectively.

we observe generally lower CSR scores across consumer-sensitive industries. Although not reported, it is noteworthy to add that firm size and R&D are positively related to CSR, whereas we observe a negative association with risk and leverage.

5 | DISCUSSION

Our study adds to the recent literature highlighting the insurance provision of CSR (Luo et al., 2018; Shiu & Yang, 2017) in relation to cyber security incidents. Motivated by the rapidly increasing threats posed to businesses worldwide, we provide novel insights regarding the context dependency of the insurance mechanism provided by CSR. In particular, we show that data breaches have important negative ramifications for breached firms in the year after a breach. We observe a significant reduction in firm profitability. However, our results indicate that CSR can play an important role in mitigating these negative consequences.

As they are associated with an increased reservoir of goodwill, a strong CSR profile can alleviate the negative implications of threatening events such as data breaches. Indeed, we show that low CSR firms suffer more severely from data breaches than firms with high CSR scores. The latter tend to enjoy higher performance (profitability) in the aftermath of a breach, indicating the value of CSR as a risk management strategy. We conclude that as data breaches become more prevalent, the need to focus on CSR, particularly in consumer-sensitive industries, also increases.

We further assess why firms might seek to adjust their CSR strategy in the post-crisis period. We posit that increasing CSR activities can help positively alter a stakeholder's assessment, especially if a crisis is seen as external, temporary, and outside of the control of the firm (Klein & Dawar, 2004; Koh et al., 2014). We provide evidence that firms utilize CSR as a remediation tool and observe that firms increase their CSR engagement after a data breach.

We further argue that industries with close consumer ties (Lev et al., 2010) are not only better structured to inhibit misconduct but are also more attuned to the implications resulting from a breach. Indeed, we reveal that data breaches do not carry uniform performance implications across firms. We find that firms that operate in consumer-sensitive industries are most affected by a breach. Our results support the view that in highly consumer-centric business environments, key stakeholders, in this case consumers, determine the insurance provision of CSR. In the context of cyber security and data protection, the negative performance implications could result from a heightened demand for trust extended to firms handling consumer information, resulting in a stronger reaction once this consumer trust is violated.

Our results further indicate that firms in consumer-centric environments actively address the loss in stakeholder trust by increasing CSR investment in the years following a data breach. Our results are in line with related studies showing that firms try to rebuild damaged stakeholder relations (Assiouras et al., 2013; Vassilikopoulou et al., 2009). Addressing stakeholders also allows the firm to portray the incident as temporary, external and outside the firm's control (Minor & Morgan, 2011; Klein & Dawar, 2004; Koh et al., 2014), reinforcing stakeholder belief that the incident does not present a threat to the survival of the firm or its long-term performance.

6 | CONCLUSION

Previous literature has highlighted a selection of benefits of incorporating ethical considerations into risk analysis frameworks (Hansson & Aven, 2014; Rozell, 2018; Ruckelshaus, 1984). In this study, we contribute to the literature by highlighting the industry-specific nature of CSR and corporate financial performance (CSR-CFP) in relation to a critical firm-specific event, a cyber security breach. Using a large cross-section of US firms affected by a total of 230 data breaches, we find evidence in support of the insurance provision of CSR in preserving corporate reputation and ultimately firm financial performance.

We specifically observe that firms with a stronger CSR profile can better alleviate the negative implications of such a threatening event. High CSR scores result in firms being less scrutinized by stakeholders over negative firm-specific events. We further observe an industry-specific provision of the CSR insurance hypothesis. More specifically, we find that in consumer-sensitive industries, high levels of CSR activities are paramount for preserving firm reputation and performance. Furthermore, we observe a tendency for firms in high consumer-sensitive industries to increase CSR activities in the aftermath of a data breach. We interpret this as an attempt to recover goodwill and alter the perception of the firm. In light of these results, while acknowledging that complete protection against all internal and external cyber threats is unrealistic (Mazzoccoli & Naldi, 2020; Paté-Cornell et al., 2018; Zheng & Albert, 2019), we conclude that managers should increase their focus on CSR as data breaches become more prevalent. This is particularly important in consumer-sensitive industries and in stakeholder scenarios where the data breach is seen as external, temporary, and outside of the control of the firm (Koh et al., 2014).

In future work, scholars could focus on the impact of a cyber security breach in related insurance-like contexts (Godfrey et al., 2009; Klein & Dawar, 2004; Li et al., 2019), by studying if CSR can reduce the public outcry and reputational backlash caused by a cyber security breach, or if corporate political activity can also limit the fallout of the breach (Hadani et al., 2019). Furthermore, given the current lack of unified disclosure requirements, the different regulatory environments across US states also offer an interesting setting to shed light on the interplay between disclosure, shareholder, or consumer reactions and the importance firms assign to cyber-related risks. In particular, consumer-level responses to data breaches could offer a rich empirical setting for policy- and legislation-relevant research, with a key question being whether or not consumers would benefit from disclosure requirements at the national level.

REFERENCES

Assiouras, I., Ozgen, O., & Skourtis, G. (2013). The impact of corporate social responsibility in food industry in product-harm crises. *British Food Journal*, *115*(1), 108–123.

Awaysheh, A., Heron, R. A., Perry, T., & Wilson, J. I. (2020). On the relation between corporate social responsibility and financial performance. *Strategic Management Journal*, *41*(6), 965–987.

Baghersad, M., & Zobel, C. W. (2022). Organizational resilience to disruption risks: Developing metrics and testing effectiveness of operational strategies. *Risk Analysis*, *42*(3), 561–579.

Barnett, M. L., Hartmann, J., & Salomon, R. M. (2018). Have you been served? Extending the relationship between corporate social responsibility and lawsuits. *Academy of Management Discoveries*, *4*(2), 109–126.

Busch, T., & Schnippering, M. (2022). Corporate social and financial performance: Revisiting the role of innovation. *Corporate Social Responsibility and Environmental Management*, *29*(3), 635–645.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643–1669.

Campbell, J. L. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. *Academy of Management Review*, *32*(3), 946–967.

Chen, X., Chen, X., Xu, L., & Wen, F. (2022). Attention to climate change and downside risk: Evidence from China. *Risk Analysis*.

Cheng, B., Ioannou, I., & Serafeim, G. (2014). Corporate social responsibility and access to finance. *Strategic Management Journal*, *35*(1), 1–23.

Christensen, S. L., & Kohls, J. (2003). Ethical decision making in times of organizational crisis: A framework for analysis. *Business & Society*, *42*(3), 328–358.

Dabic, M., Colovic, A., Lamotte, O., Painter-Morland, M., & Brozovic, S. (2016). Industry-specific CSR: Analysis of 20 years of research. *European Business Review*, *28*(3), 250–273.

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27–55.

Doh, J. P., & Guay, T. R. (2006). Corporate social responsibility, public policy, and NGO activism in Europe and the United States: An institutional-stakeholder perspective. *Journal of Management Studies*, *43*(1), 47–73.

Eling, M., & Jung, K. (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics*, *82*, 167–180.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585.

Figuié, M., & Fournier, T. (2008). Avian influenza in Vietnam: Chicken-hearted consumers? *Risk Analysis*, *28*(2), 441–451.

Friede, G., Busch, T., & Bassen, A. (2015). ESG and financial performance: Aggregated evidence from more than 2000 empirical studies. *Journal of Sustainable Finance & Investment*, *5*(4), 210–233.

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

Hadani, M., Doh, J. P., & Schneider, M. (2019). Social movements and corporate political activity: Managerial responses to socially oriented shareholder activism. *Journal of Business Research*, *95*, 156–170.

Hansson, S. O., & Aven, T. (2014). Is risk analysis scientific? *Risk Analysis*, *34*(7), 1173–1183.

Hashemi, S. J., Khan, F., & Ahmed, S. (2019). An insurance model for risk management of process facilities. *Risk Analysis*, *39*(3), 713–728.

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

Jian, M., & Lee, K.-W. (2015). CEO compensation and corporate social responsibility. *Journal of Multinational Financial Management*, *29*, 46–65.

Jo, H., & Harjoto, M. A. (2012). The causal effect of corporate governance on corporate social responsibility. *Journal of Business Ethics*, *106*(1), 53–72.

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.

Kim, Y., Park, H., & Kim, J. K. (2019). Corporate association strategies and consumer responses: The relative effectiveness of CA versus CSR communication strategy by industry type. *Journal of Marketing Communications*, *25*(2), 204–227.

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

Knight, R., & Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers Security*, *99*, 102036.

Koh, P.-S., Qian, C., & Wang, H. (2014). Firm litigation risk and the insurance value of corporate social performance. *Strategic Management Journal*, *35*(10), 1464–1482.

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

Lev, B., Petrovits, C., & Radhakrishnan, S. (2010). Is doing good good for you? How corporate charitable contributions enhance revenue growth. *Strategic Management Journal*, *31*(2), 182–200.

Lev, B., & Radhakrishnan, S. (2005). The valuation of organization capital. *Measuring capital in the new economy* (pp. 73–110). University of Chicago Press.

Li, W., Lu, Y., & Li, W. (2019). Does CSR action provide insurance-like protection to tax-avoiding firms? Evidence from China. *Sustainability*, *11*(19), 5297.

Lins, K. V., Servaes, H., & Tamayo, A. (2017). Social capital, trust, and firm performance: The value of corporate social responsibility during the financial crisis. *Journal of Finance*, *72*(4), 1785–1824.

Löfstedt, R. E., & Renn, O. (1997). The brent spar controversy: An example of risk communication gone wrong. *Risk Analysis*, *17*(2), 131–136.

Luo, J., Kaul, A., & Seo, H. (2018). Winning us with trifles: Adverse selection in the use of philanthropy as insurance. *Strategic Management Journal*, *39*(10), 2591–2617.

Luo, J., Meier, S., & Oberholzer-Gee, F. (2013). No news is good news: CSR strategy and newspaper coverage of negative firm events. *Working Paper*. https://hbswk.hbs.edu/item/no-news-is-good-news-csr-strategy-and-newspaper-coverage-of-negative-firm-events

Mazzoccoli, A., & Naldi, M. (2020). Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Analysis*, *40*(3), 550–564.

Minor, D., & Morgan, J. (2011). CSR as reputation insurance: Primum non nocere. *California Management Review*, *53*(3), 40–59.

Mishra, D. R. (2017). Post-innovation CSR performance and firm value. *Journal of Business Ethics*, *140*(2), 285–306.

Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226–241.

Peloza, J. (2006). Using corporate social responsibility as insurance for financial performance. *California Management Review*, *48*(2), 52–72.

Peters, R. H., & Taylor, L. A. (2017). Intangible capital and the investment-q relation. *Journal of Financial Economics*, *123*(2), 251–272.

Petrenko, O. V., Aime, F., Ridge, J., & Hill, A. (2016). Corporate social responsibility or CEO narcissism? CSR motivations and organizational performance. *Strategic Management Journal*, *37*(2), 262–279.

Pfarrer, M. D., Decelles, K. A., Smith, K. G., & Taylor, M. S. (2008). After the fall: Reintegrating the corrupt organization. *Academy of Management Review*, *33*(3), 730–749.

Ponemon Institute. (2022). *IBM cost of a data breach report 2022 (Tech. Rep.)*. Ponemon Institute. http://www.ibm.com/security/data-breach

Rozell, D. J. (2018). The ethical foundations of risk analysis. *Risk Analysis*, *38*(8), 1529–1533.

Ruckelshaus, W. D. (1984). Risk in a free society. *Environmental Law Reporter News & Analysis*, *14*, 10190.

Schnietz, K. E., & Epstein, M. J. (2005). Exploring the financial value of a reputation for corporate social responsibility during a crisis. *Corporate Reputation Review*, *7*(4), 327–345.

Sellnow, T. L., Sellnow, D. D., Lane, D. R., & Littlefield, R. S. (2012). The value of instructional communication in crisis situations: Restoring order to chaos. *Risk Analysis*, *32*(4), 633–643.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341.

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

Shiu, Y.-M., & Yang, S.-L. (2017). Does engagement in corporate social responsibility provide strategic insurance-like effects? *Strategic Management Journal*, *38*(2), 455–470.

Shrivastava, P. (1993). Crisis theory/practice: Towards a sustainable future. *Industrial & Environmental Crisis Quarterly*, *7*(1), 23–42.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795.

Ulmer, R. R., & Sellnow, T. L. (2000). Consistent questions of ambiguity in organizational crisis communication: Jack in the box as a case study. *Journal of Business Ethics*, *25*(2), 143–155.

Vassilikopoulou, A., Siomkos, G., Chatzipanagiotou, K., & Pantouvakis, A. (2009). Product-harm crisis management: Time heals all wounds? *Journal of Retailing and Consumer Services*, *16*(3), 174–180.

Velte, P. (2021). Meta-analyses on corporate social responsibility (CSR): A literature review. *Management Review Quarterly*, *72*, 627–675.

Wang, Q., Dou, J., & Jia, S. (2016). A meta-analytic review of corporate social responsibility and corporate financial performance: The moderating effect of contextual factors. *Business & Society*, *55*(8), 1083–1121.

Wei, J., Zhao, M., Wang, F., Cheng, P., & Zhao, D. (2016). An empirical study of the Volkswagen crisis in China: Customers' information processing and behavioral intentions. *Risk Analysis*, *36*(1), 114–129.

Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis*, *42*(8), 1606–1622.

Zheng, K., & Albert, L. A. (2019). A robust approach for mitigating risks in cyber supply chains. *Risk Analysis*, *39*(9), 2076–2092.

How to cite this article: Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., & Vigne, S. (2023). Are the good spared? Corporate social responsibility as insurance against cyber security incidents. *Risk Analysis*, 1–16. https://doi.org/10.1111/risa.14122

APPENDIX

TABLE A1 Variable descriptions. This table provides variable definitions for the main variables used throughout this study. We provide variable names, variable descriptions, and data sources

Variables	Variable description	Source
CSR_score	The difference between CSR strengths and CSR concerns	MSCI ESG Stats (formerly known as KLD)
CSR_score(Gov)	The difference between CSR strengths and CSR concerns including the corporate governance category	MSCI ESG Stats (formerly known as KLD)
Consumer-sensitive_industry	Consumer goods companies (SIC codes: 0000–0999, 2000–2399, 2500–2599, 2700–2799, 2830–2869, 3000–3219, 3420–3429, 3523, 3600–3669, 3700–3719, 3751, 3850–3879, 3880–3999, 4813, 4830–4899, 5000–5079, 5090–5099, 5130–5159, 5220–5999, 7000–7299, and 7400–9999) and finance companies with SIC codes: 6000–6999)	Compustat
Data_breach	Indicator variable equal to 1 if a firm suffered a data breach in a given year; 0 otherwise. Examples of breaches classified by the PRC include incidents due to credit/debit card fraud; hacks by malware or a malicious outside party; malicious insiders; lost, discarded, or stolen physical devices, documents, laptops, smartphones, memory sticks, and hard-drives; and unintended disclosures of sensitive information.	Privacy Rights Clearinghouse
ROA	Return on Assets: Net income/Total assets	Compustat
ROE	Return on Equity: Net income/Market value of equity	Compustat
ROS	Return on Sales: Operating profit/Net sales	Compustat
Tobins_Q	(Total assets + Market value – Total common equity)/Total assets	Compustat
R&D	R&D expenditure/Total assets	Compustat
Intangibles	(30% of selling, general and administrative expenses + R&D expenses)/Total assets	Compustat
Size	Total assets	Compustat
Market-to-book	(Market value of equity + Total debt + Preferred stock – Deferred taxes and Investment tax credit)/Total assets	Compustat
Stock_return	Holding period stock return over the fiscal year	CRSP
Risk	Standard deviation of daily stock return for the fiscal year	CRSP
Dividend	Indicator variable equal to 1 if a firm pays cash dividends on common equity, and 0 otherwise.	Compustat
Leverage	(Long-term debt + Debt in current liabilities)/Total assets	Compustat

TABLE A2 Data breaches, CSR, and alternative profitability measures. This table reports the results of linear regression models using various profitability measures as the dependent variable (ROE, ROS, and Tobins_Q). *Data_breach* is an indicator variable equal to 1 if the firm suffered a data breach and 0 otherwise. *CSR_score* is the firm's CSR score computed based on KLD data. The variable of interest is the interaction term *Data_breach* × *CSR_score*. All explanatory variables are lagged by one time period

ROE

	(1)	**(2)**	**(3)**	**(4)**
Data_breach$_{(t-1)}$	−0.011*	−0.011**	−0.012*	−0.012**
	(−1.84)	(−2.30)	(−1.86)	(−2.18)
CSR_score$_{(t-1)}$	−0.001	−0.000	0.000	0.001
	(−0.13)	(−0.05)	(−0.06)	(0.13)
Data_breach$_{(t-1)}$ × *CSR Score*$_{(t-1)}$	0.005*	0.005**	0.005*	0.005**
	(1.85)	(2.06)	(1.90)	(2.07)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	5092	5092	5092	5092
R^2	0.067	0.068	0.096	0.095

ROS

	(1)	**(2)**	**(3)**	**(4)**
Data_breach$_{(t-1)}$	−0.044**	−0.040**	−0.038**	−0.037**
	(−2.24)	(−2.20)	(−2.19)	(−2.18)
CSR_score$_{(t-1)}$	0.002	0.003	0.002	0.002
	(1.12)	(1.36)	(1.03)	(1.16)
Data_breach$_{(t-1)}$ × *CSR_score*$_{(t-1)}$	0.005*	0.005*	0.004*	0.004*
	(1.87)	(1.85)	(1.84)	(1.84)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	5092	5092	5092	5092
R^2	0.073	0.088	0.092	0.097

Tobins_Q

	(1)	**(2)**	**(3)**	**(4)**
Data_breach$_{(t-1)}$	0.040	0.036	0.040	0.037
	(0.89)	(0.81)	(0.88)	(0.83)
CSR_score$_{(t-1)}$	0.000	−0.000	−0.001	−0.001
	(0.01)	(−0.12)	(−0.19)	(−0.37)
Data_breach$_{(t-1)}$ × *CSR_score*$_{(t-1)}$	0.004*	0.003*	0.004*	0.004
	(1.88)	(1.84)	(1.93)	(1.68)
Control for R&D	Yes	No	Yes	No
Control for Intangibles	No	Yes	No	Yes
Control Variables (see Table 4)	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Industry FE	No	No	Yes	Yes
Observations	5092	5092	5092	5092
R^2	0.073	0.073	0.078	0.078

Note: *t*-Statistics given in parentheses are based on standard errors corrected for heteroskedasticity and firm-level clustering. Asterisks ***, **, and * indicate statistical significance at 1%, 5%, and 10% levels, respectively.