We Care About Your Privacy (When It Matters): How Firms Strategically Respond to Data Breach Incidents

by

Ji Young Huh

Business Administration
Duke University

Date:_____

Approved:

_____
Allison Chaney, Supervisor

_____
Christine Moorman

_____
Tong Guo

Thesis submitted in partial fulfillment of
the requirements for the degree of Master of Arts
in Business Administration in the Graduate School of Duke University

2022

ABSTRACT

We Care About Your Privacy (When It Matters):
How Firms Strategically Respond to Data Breach Incidents

by

Ji Young Huh

Business Administration
Duke University

Date:_____
Approved:

_____
Allison Chaney, Supervisor

_____
Christine Moorman

_____
Tong Guo

An abstract of a thesis submitted in partial fulfillment of
the requirements for the degree of Master of Arts
in Business Administration in the Graduate School of Duke University

2022

Abstract

With a growing concern around consumer data and online privacy, regulators around the world are placing numerous measures to educate individuals with their privacy choices and to require firms to prioritize consumer privacy. Past studies have reported that privacy protection failure, mainly data breach incidents, negatively affects firms, but less is known about how firms change their business strategies. This paper studies how firms adjust their strategic emphasis, specifically between creating value for the consumers and appropriating value to protect their current businesses, after security incidents. Based on data breach incidents experienced by 70 US public firms from 2004 to 2014, findings show firms on average shift their strategic emphasis to fixing the problem through increasing R&D expenses relative to advertising expenses, moderated by the firms' internal and external resource profiles. The research hopes to contribute to the growing marketing literature on privacy.

Contents

List of Tables

List of Figures

1. Introduction

As data breaches become more prevalent, cybersecurity has increasingly been on firms' radar as one of the biggest threats to their businesses. For instance, Facebook (Meta) lists data security threats as one of its risk factors that would adversely affect their business,[1] and Home Depot lists privacy and security of their data could "incur substantial costs and reputational damage."[2] Along with the evolving regulatory environment, the cybersecurity market is predicted to reach over $500 billion by 2030, up from $180 billion in 2020.[3] In accord with these trends, Deloitte reported that average annual security spending per employee increased from $2,337 in 2019 to $2,691 in 2020.[4]

While firms express their concerns about cybersecurity and increase their spending in preparation for attacks, it is unclear how they respond when they experience an actual data breach. Extant literature on digital privacy focuses on the consequences of data breach on firm performance in terms firm market value (Campbell et al. 2003; Martin, Borah, and Palmatier 2017) or changes in consumer behavior (Janakiraman, Lim, and Rishika 2018; Turjeman and Feinberg 2019). However, less is studied about how firms act in response to the attack. Researchers have found companies tend to vary in how they communicate information about the breach to their customers through notification letters (Bisogni 2015) and how the communication method moderates the impact of data breach on consumers' perception on the firms (Martin, Borah, and

[1] Facebook 2021 Financial Report 10K
[2] Home Depot 2021 Financial Report 10K
[3] ResearchAndMarkets.com Industry Forecast, https://www.yahoo.com/now/global-cyber-security-market-2021- 102500547.html
[4] https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/DI_2020-FS-ISAC-Cybersecurity.pdf

Palmatier 2017). Nonetheless, these papers do not study how firms adjust their business strategies in response to data breach incidents.

This paper studies how firms respond to data breaches by adjusting their spending. Under dynamic capabilities theory, firms should ideally adapt to an unforeseen change by adjusting their strategies to utilize their resources in a way that better fits and manages the threat (Teece, Pisano, and Shuen 1997). Consistent with this view, the literature on product harm crises finds that companies that respond quickly and actively to fix the underlying problems fare the best (Eilert et al. 2017). However, given the longer-term and uncertain negative impact of data breach incidents, it is not clear how companies will react.

I further introduce the firms' resource profiles to explain the heterogeneity across their responses to external threats. Each firm differs in its resources. Some of the resources are owned by the firm, such as a strong brand or business size. Other resources are available in the environment by the virtue of where the firm chooses to compete. Based on different abundant or constrained capacities, I propose that firm and industry resources will moderate how managers take one of two possible actions. On the one hand, managers can actively address the potential causes and concerns for the data breach by strengthening their security systems, hiring new human resources for improved surveillance, or developing future products and services that are more sensitive or would minimize harms such attacks. On the other hand, managers can seek to bolster their company's reputations against the harm caused by the breach while maintaining their current businesses. The first course of action could be viewed as creating value through efforts to actively fix the problem, while the second can be viewed as appropriating value

from their current businesses by protecting and advocating for them. I propose firm resources determine their individual strategic decisions. Some resources could attract more scrutiny from outside to fix the problem, while other resources could motivate firms to stay on their status quo and focus on temporary responses. I investigate whether and to what extent firm and industry resources will moderate whether and how a firm responds to a data breach incident. Specifically, I examine whether resources influence a firm's tendency to respond to a data breach by exploring new strategies in order to create more value or by trying to protect and appropriate value from their current business. Considering that recent privacy regulations, from disclosure laws to data processing requirements, urge firms to become proactive in protecting their customers from data breach, understanding circumstances that would lead firms to divert their efforts from focusing on the problems would be relevant.

This paper is structured as follows. The remainder of this section reviews what has been studied about digital privacy and discusses why I use strategic emphasis on value appropriation to measure firms' strategic response. I present a theoretical framework to explain how and why data breach would affect firm spending, and hypotheses on how different resources will alter the impact. Data section illustrates further on the data used for analyses, followed by the model and results. I conclude with a discussion and limitations.

1.1 Data Breach as a Privacy Threat

Motivation for this research stems from the uniqueness of privacy concerns as an external threat, as data breach does not generally have an immediate and apparent harm on consumers unlike other firm crises such as product failure where victims and their

losses are clear. When a firm experiences a product failure, consumers who purchased the products are the victims and the losses are determined by the prices paid as well as the harm created by the defect. On the contrary, when a firm experiences a data breach, it is only possible to identify who is potentially involved without knowing when and how the breached information will be misused in the future, if at all. Making things even less clear, the breached information is most likely shared by various other firms; therefore, even if a consumer suffers from a cybercrime like an identity theft, the actual source of identity loss cannot be traced.

Given these differences, consumers do not adversely react to data breach incidents as they do to other crises (Acquisti, Taylor, and Wagman 2016; Athey, Catalini, and Tucker 2017). For instance, fewer than 1% of the consumers asked for a credit freeze after the Equifax data breach, which was highly recommended to almost half of the population in the country (Cole 2017). Due to the lack of clarity in the victims, harms, and responsibilities, proving privacy harms in lawsuits has also been difficult (Citron and Solove 2021; Solove and Citron 2018), further weakening the urgency posed by the security risks associated with data breach.

Table 1 summarizes the extant literature that examine the impact of data breach. What these papers study can be broken down into three broad categories: consumer consequences in terms of financial loss or changes in behaviors; firm performance consequences, both financially and reputationally; and firms' responses, focused mainly on communications. The majority of research focus on firm performances and consumer responses, and even for the few that look at firm responses, they look at firms' responses as the independent variable. Bisogni (2015) provides descriptive analyses on breach

notification letters and investigates how they vary in responding and communicating regarding the incidents. The research finds the letters vary in the level of transparency and message types, and they tend to belittle the event when the firms were found to be responsible for the incidents. Gwebu, Wang, and Wang (2018) investigates how different response strategies—accommodative, moderate, defensive, and image renewal strategies—augment or lessen the negative impact of data breach on the firm's market value. I noticed that there is a lack of understanding on how firms adapt to these privacy threats. This paper is an attempt to address the gap by investigating one aspect of which firms could possibly transform, which is their strategic focus between value appropriation and value creation.

I further investigate the heterogeneity in firms' responses to data breach using their internal and external resources. Malhotra and Malhotra (2011) find firm size and breach magnitude moderate the impact of data breach on stock performances. This paper incorporates factors that are based on resources that firms have, such as brand value, marketing insights, and market foreseeability, to explain heterogeneity in the impact of data breach on firms' responses with strategic decisions.

Unlike previous literature where firms are compared against each other, I compare shifts in strategic emphasis within the firms before and after data breach. Controlling for the different determinants of strategic emphasis, I introduce firm and industry resources that would moderate the impact of data breach on firms strategizing around creating values by facing the problem versus appropriating value by protecting their current businesses that might leave their consumers more vulnerable.

Table 1: Literature on Data Breach

Relevance	Findings from the literature
Impact of Data Breach on the Firm's Stock Performance	Market responds negatively to a data breach (Acquisti, Friedman, and Telang 2006), especially when it involves confidential information (Campbell et al. 2003) or large number of records (Malhotra and Malhotra 2011)
	Positive news bundling can offset negative impact of a data breach on the firm's stock price (Gay 2017)
	Data breach at a firm negatively affects market value of its competitors (Kashmiri, Nicol, and Hsu 2017); severity of the breach positively affects the competitors (Martin et al. 2018)
	Negative stock responses are attenuated by the amount of news pressure at the time of the announcement (Foerderer and Schuetz 2022)
Impact of Data Breach on the Firm other than Stock Performance	Costs associated with cybercrimes have significantly increased (Anderson et al. 2019)
	Data breach damages the firm's reputation (Makridis 2021)
	Data breach weakens the firm's brand capital (Hsu, Kao, and Wang 2021)
	Data breach negatively affects the firm's bank loan terms (Huang and Wang 2021)
Impact of Data Breach on Consumer Responses	When a multichannel retailer experiences a data breach at one channel, consumers shift their business to an unbreached channels of the retailer (Janakiraman, Lim, and Rishika 2018)
	Consumers significantly reduce their information sharing on the firm's platform to avoid personal identification after data breach (Turjeman and Feinberg 2019)
	Data breach increases privacy protection behaviors from the consumers through stress and social contract violations (Labrecque et al. 2021)
Firm Responses to Data Breach	Firms employ various strategies with message types when they notify their customers about data breach (Bisogni 2015)
	Response strategies deliver different effectiveness in managing the crisis, where the efficacy depends on the firm reputation (Gwebu, Wang, and Wang 2018)

1.2 Strategic Emphasis on Appropriating vs. Creating Value

Strategic focus between value appropriation and value creation has been studied in the field of marketing, expressed by (ad expenses – R&D expenses)/assets ratio.

Strategic emphasis was studied for its financial implications (Mizik and Jacobson 2003), its association with merger motives (Swaminathan, Murshed, and Hulland 2008), and its impact on firm risks (Han, Mittal, and Zhang 2017). The same measure is also interpreted as marketing ambidexterity by Josephson, Johnson, and Mariadoss (2016) between exploitation of existing businesses (i.e., value appropriation) and exploration (i.e., value creation) of future opportunities. Strategic emphasis is a relevant measure for my purpose of this paper, as I am interested in firms, after data breach, (1) addressing privacy concerns through dedicated measures to integrate privacy protection within their businesses and create value, and (2) communicating with the consumers to repair the temporal reputational damage to appropriate value.

Previous literature examines firm characteristics and industry contexts to be key determinants of the firms' strategic emphases. In this paper, I study strategic emphases as an investment tradeoff companies make between appropriating value from its current business and creating value with new strategic directions. In the context of data breach, this tradeoff is between advertising investments to bolster the company's reputation versus R&D investments to solve the causes that might be associated with breach weakness or to build a better system resilient to similar attacks. I characterize this choice as "strategic" in the economic sense (Mizik and Jacobson 2003) because the choice to bolster reputation is not a choice focused on solving the underlying problem for consumers, but instead, on a calculus that it is better for the firm to deflect attention away from the problem given current resource positions. This view is consistent with the finding in Wies et al. (2019) that firms increase advertising spending to improve perception when faced with complaints.

Studying firms' strategic responses to data breach is important for three reasons. First, it teaches us whether data breach has a substantive impact on the firm's business strategy. Firm responses like data breach notification strategies or changes in privacy policies are to communicate with its consumers and address their privacy concerns. Strategic emphasis on whether to invest in solving the problem or bolstering reputation, however, illustrates how firms internally decide on managing their businesses. Changes in business emphasis represent the consequences of data breach on firms to a fuller extent, which will help firms to more accurately perform risk analyses of the attacks. Secondly, learning about the firms' adjustment of strategic focus would contribute to the evaluation of privacy regulations. In assessing privacy harms, impact of data breach on how firms decide to allocate their resources to extract profits or to create values would demonstrate a more fundamental picture of how firms respond to privacy incidents. With more privacy regulations getting proposed and passed, it is crucial for policymakers to consider how firms are affected by privacy incidents, and studying data breach will be a starting step of broadening our understanding. In addition, the findings on how firms' resources moderate these impacts present possibilities of disproportionate magnitude of privacy threats on firms. This would be in line with previous research on brand trust moderating the impact of data breach on consumers (Martin, Borah, and Palmatier 2017) and adverse impact on small firms from privacy regulations (Johnson and Shriver 2020). Then, both firms and policymakers could use the findings in assessing privacy threats.

2. Theoretical Framework

Upon realizing it was involved in a cybersecurity attack, a firm could first spend its resources to investigate the source the attack, and address the problem to prevent or mitigate the impact of future potential attacks. It could revamp their maintenance or auditing protocols to reduce harms, and it could also invest in products or services that will minimize the harm if there were to be another incident in the future. Google, for instance, is investing in Privacy Sandbox in response to the growing concern on privacy threats and industry changes, anticipating privacy regulations to emerge. The firm could also try to distract the consumers from the incidents and build brand images instead. It could launch more aggressive campaigns to renew their images or offer complimentary services or price discounts to recover their reputations.

In this section, I first propose that on average, firms try to fix their problems after data breach. Then, I consider different resources available to the firms that might heterogeneously affect their strategic decisions: resources that firms own, such as brand equity, market size, and marketing insights, and resources determined by the industry that the firm operates in, such as market certainty, industry knowledge about data breach, and competition intensity. **Figure 1** illustrates the individual effects of these resources.

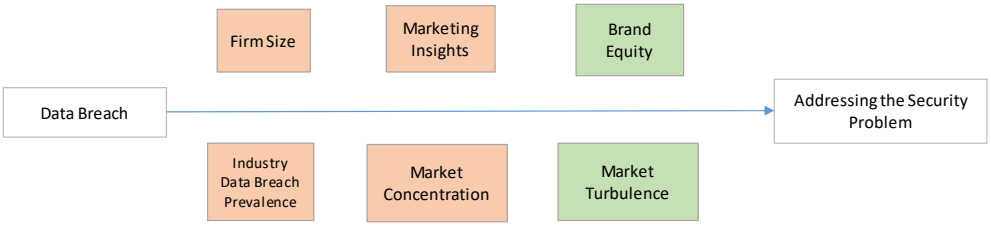

Figure 1: Framework Overview

2.1 Main Effect

I first hypothesize that data breach will incentivize firms to increase their emphasis on value creation (relative to value appropriation) for two main reasons arising from the unique characteristics of data breach. First, firms lack motivation to communicate with consumers to persuade them since consumers do not "care" enough to take actions; secondly, firms face pressure from the regulatory environment urging firms to develop privacy-friendly strategies. I elaborate on both below.

Firms will be less incentivized to explore new business strategies because consumers are unlikely to take actions or change behaviors after data breach. Recent studies find individuals do not act upon learning about a data breach by which they might have been affected. A data breach at a matchmaking website caused a modest, short-lasting reduction in consumer activities (Turjeman and Feinberg 2019), and Alipay users' privacy concerns did not alter their privacy settings (Chen et al. 2021). This is consistent with what privacy scholars find, often referred to as a privacy paradox---unlike the prevalent anxiety over privacy concerns, individuals do not act to protect their privacy

(Acquisti, Taylor, and Wagman 2016; Athey, Catalini, and Tucker 2017). As consumers show lack of action towards protecting privacy after data breach, communicating to the consumers about the threats or to defend themselves from the potential threat will not appeal to the firms as necessary or beneficial.

On the other hand, firms have incentives to solve the problems as regulations around data breach and online privacy have been rapidly evolving in recent years. With EU and California setting precedents, various states within the United States have enacted or are in the process of drafting privacy laws. While they vary in scope and terms, the primary goal of the regulations is to give privacy control to individuals as well as to protect their data online. By investing in future opportunities that will be more resilient to future privacy threats while protecting consumers and comply by the regulations, firms can lead on reducing costs from privacy harms as well as compliance costs. Furthermore, firms have incentives to focus on creating values for customers in the future because prospective new businesses could also dissipate negative impact of data breach (Gay 2017), protecting the firm from any additional damages.

With a lack of urgency to distract consumers from the issue and incentives to address the problems that would be compliant with the privacy-centric regulatory changes, I hypothesize that security incidents will encourage firms to invest in developing more secure products and services to protect consumers and minimize potential damages in the future, as well as modifying business strategies to adopt to regulatory changes.

H1. On average, firms focus on addressing the problem posed by data breach.

While I hypothesize firms will increase their emphasis on creating values for the customers by addressing the privacy concerns, I also believe firms' strategic responses will be heavily influenced by resources they have available. Consequently, the main effect without considering the heterogeneity from resource profiles may result in lack of statistical significance.

2.2 The Impact of Firm-level Resources

Resource-based view and dynamic capabilities theory in strategy both acknowledge resources to be the key in forming a firm's competitive advantage. While they differ in how firms manage to sustain the competences from the resources, it is widely accepted that firms develop and form decisions based on those resources that firms have access to. In this section, I adopt the view of dynamic capabilities theories, and demonstrate firms can integrate and adjust their competences in the face of data breach based on their internal resource profiles.

Firm size: An important resource of a firm is its human capital. Firms with more employees share more ideas and experiences, has bandwidth to manage multiple projects, and subdivide responsibilities for increased efficiency. There are more varieties of goals and priorities that security concerns would have to compete with, both in terms of budgeting but also making business decisions. Especially since value creation determines and represents the core and the purpose of a business (Mizik and Jacobson 2003), making strategic decisions to invest in privacy protective opportunities will be more difficult with big and established firms. For instance, appropriating value through marketing and advertising can be discussed and carried out within a marketing department, but creating value through pursuing new business opportunities requires more administrative

procedures as it is more central to the business operation that would impact all parts of the firm, leading to a delay in the process. Therefore, firms of bigger sizes will be less likely to respond to a security breach by addressing privacy concerns in its business strategies compared to smaller firms. This is in part consistent with past literature which finds the adverse impact of company size on innovations (Chandy and Tellis 2000). Instead, it will seek for a temporary solution from interacting with the consumers about their privacy measures to alleviate their concerns.

H2: Big firms are more likely to focus on distracting consumers' attentions from data breach harms rather than on addressing the privacy concerns.

Marketing insights: Intellectual resources are also invaluable to firms. Among various expertise, marketing insights are particularly relevant in making strategic decisions between interacting with existing customers and finding valuable opportunities to attract new customers. Role of a Chief Marketing Officer (CMO) includes identifying new market opportunities and associated threats, contributing customer perspective for firm decisions, and managing its relationship with its consumers (Boyd, Chandy, and Cunha 2010). Their responsibilities involve interacting with the consumers, both existing and potential, and managing the relationships with them. Germann, Ebbes, and Grewal (2015) employ a variety of model specifications to show that the presence of CMO has a positive impact on firms' performances. When facing a data breach, firms with marketing expertise in their management team would respond more sensitively to communicate with their existing customers as well as future customers. Because their tools are more closely related with appropriating business values than creating new values, strategic emphases will be more likely to be transferred to advertising expenses than research expenses.

H3: Marketing insights at a firm encourage communicating with its consumers rather than addressing the problems

Brand equity: Brand equity has been studied as an important resource to firms. Consumers hold positive impressions about the firm and its products or services with high brand value (Lane 1991; Shocker and Aaker 1993). As Hsu, Kao, and Wang (2021) reports that cybersecurity attacks hurt brand capital, firms with strong brand values perceive a data breach incident to be a major threat to their businesses, taking the problem more seriously, thus increasing emphasis on creating values from privacy protective businesses. Furthermore, previous literature on crisis management finds positive correlation between brand equity and marketing effectiveness after crises (Zhao, Zhao, and Helsen 2011). Considering data breach as a crisis, firms with strong brand equity would require less efforts in marketing compared to those with weak brand equity for the same extent of impact, and thus will be more likely to devote attention to fixing the problem than to recover their reputation. For these reasons, I hypothesize that a firm with stronger brand equity will be more likely to focus on trying to prevent privacy violations in the future.

H4: Brand equity provides resilience to crises and facilitates firms to focus on fixing security problems.

2.3 The Impact of Industry-level Resources

Unlike firm-level resources that firms own or develop internally, industry-level resources are often externally determined by competitors, market forces, or other non-controllable factors. Industry prospects and characteristics can provide (or deprive)

invaluable informational resources that could help firms navigate through crises with clarity, predictability, or caution. As noted in 1.1, data breach poses a unique threat to consumers because of the difficulty to forecast consumer backlash. Information resources can be valuable to firms in deciding whether to focus on solving the problem or communicate with the consumers.

Prevalence of data breach in the industry: One type of information firms can obtain from their surroundings is specifically about data breach. Some industries are more exposed to data breach incidents than others, and when they do, all players in the industries are affected. When Target had its big data breach incident in 2013, it had negative spillover effects on its competitors' stock performances, with larger negative impact for firms more similar to Target (Kashmiri, Nicol, and Hsu 2017). Public is more aware of the privacy concerns in the industry, making it more likely for the firms to expect bigger criticisms after data breach incidents. I consider this to be an industry resource which firm can use to better predict the consequences of its data breach and adjust their strategies accordingly. Data breach prevalence will raise the public's awareness of privacy concerns, motivating firms to actively engage in communication with their consumers and to recover from the reputational harm to follow.

H5: Data breach prevalence in the industry intensifies privacy concerns among the consumers, encouraging the firm to repair likely reputational damages rather than directly addressing them.

Market Concentration: When markets are not concentrated, firms face competition from other firms. This rivalry puts pressure on firms to resolve problems when they arise, such as data breach, as their competitors will be eager to take advantage

of their misfortunes. The knowledge about how their competitors will react functions as an informational resource that motivates firms to more actively resolve the problem. In other words, firms in a competitive market will be likely to resolve the problem and explore future opportunities to maintain their competitive advantage. On the other hand, when the industry knowledge reveals that the market is concentrated and there is not much pressure to resolve the issue, they could rather focus on comforting their consumers.

H6: In a concentrated market, firms do not face high competition, weakening their need to fix the problems posed by data breach.

Market turbulence: Market turbulence refers to the rate of change in the market, such as consumers' tastes and technologies. According to contingency theory, the business environment is as important as the business strategy itself in driving its performance (Donaldson 2001). Market turbulence affects informational resources about the predictability of its businesses in the industry. When the market is turbulent and its sales are not stable, forecasting upcoming performances of new projects or even current projects in the close future becomes challenging (Challagalla, Murtha, and Jaworski 2014). Consequently, the uncertainty about consumers' responses for data breach will also be exacerbated. Further decreased clarity of firms' assessment of consumer privacy harms will discourage them from devoting efforts to sustain their current businesses which will remain less useful over time. Instead, I hypothesize that such lack of resources for predictability in the security crises will accelerate firms' motivation to address privacy concerns to better prevent future cyberattacks that would trigger more uncertainty.

H7: Market turbulence lessens firms' predictability of their business strategies, encouraging them to address the privacy concerns by investing in future opportunities that would protect themselves from future privacy attacks.

2.4 Evaluating Data Breach Incidents

While data breach incidents indicate vulnerability in the firms' security systems, they pose differential threats to firms depending on the details about the incidents, such as how the breach took place, what was involved, and how many individuals are affected. For instance, an incident involving a laptop lost for a couple of hours by mistake will be significantly different from a ransomware attack that threatened the entire business to be halted for a few hours. I hypothesize that the moderating effects will be more significant and bigger in magnitude for the incidents that are perceived to be more severe and impactful.

H8: Moderating impact of firm-level and industry-level resources on how firms respond to data breach will be strengthened with the severity of the data breach incidents.

3. Data

I conduct analyses on publicly traded firms for the period of 2004 to 2014. For each firm-year, I collect firm characteristics like number of employees, sales, and market value, as well as variables for industry-level factors like market turbulence and concentration from Compustat. I collect brand value information from annual ranking of the Best Global Brands, published by Interbrand. Number of analysts that follow each firm is obtained from I/B/E/S dataset, which is used to proxy for market scrutiny. To collect information on how firms value marketing insights. I use Execucomp database which includes top 5 management roles with the highest compensation. I categorize firms utilizing marketing insights if marketing or consumer related positions are included in the top management roles.

Based on the company level information, I identify the data breach incidents and related information using data published by Rosati and Lynn (2021). The authors take data from Privacy Rights Clearinghouse[5] which records data breach incidents that occurred between 2005 and 2014, and attach associated company identifier and its fiscal year for each incident of data breach in the data. This dataset has been widely used in academia to study data breach (Huang and Wang 2021; Martin, Borah, and Palmatier 2017; Zou et al. 2019). To further control for different characteristics of data breach, I use number of articles about each data breach from Factiva.

[5] P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: January 2021. [Online]. Available: https://www.privacyrights.org/data-breaches.

3.1 Sample Selection

The analyses are restricted to firms incorporated and traded in the United States (available on Compustat Fundamentals Annual), with over 50,000 firm-years from over 9,000 companies from 2004 to 2014. I merge on the information about data breach incidents (Rosati and Lynn 2021) and identify 308 firm-years with data breach from 202 distinct firms. From here, I keep companies that report R&D and advertising expenses at least one year in the data. I discard if companies never report one or more of the two expenses since I do not know if the numbers are missing because companies did not have the expenses, or they simply did not report; when they are missing these values for only certain years in the data set, I interpolate using the firm's other years' ratio of each to Selling, General, and Administrative expenses (SG&A). This leaves us with around 15,000 firm-years from 2,000 firms; data breach incidents from 80 distinct firms. I then eliminate firms that never report a year of financial information necessary for the model, as well as the firms that do not appear in Execucomp database. Final dataset is consisted of 6,901 firm-years from 879 firms; data breach incidents from 70 distinct firms. **Table 2** presents the overview of sample development.

Table 2: Data Processing Steps

	Number of:	
	Firms	**Data Breach**
Total number of data breach incidents in Privacy Rights Clearinghouse data set (2005-2014)		9,015
Incidents from public firms in (Rosati and Lynn 2021)		506
Incidents that are first occurrence at a firm		259
Total number of public firms in Compustat (2004-2014)	9,269	203
Firms with data on advertising and R&D expenses	2,057	80
Firms with data on number of employees	2,010	79
Firms found on Execucomp for data on executives	923	71
Firms with data on financial information	879	70

3.2 Dependent Variable

I follow seminal work of Mizik and Jacobson (2003) for measuring firms' relative emphasis between creating and appropriating value. They define strategic emphasis for firm *i* at time *t* as:

$$\mathrm{SE_{it}} = \frac{advertising\ expense_{it} - R\&D\ expense_{it}}{assets_{it}}.$$

Advertising expenses and R&D expenses are widely employed as proxies for appropriating and creating new values, respectively (Josephson, Johnson, and Mariadoss 2016; Mizik and Jacobson 2003, 2007). By taking the difference between the two and scaling it by total assets, this measure illustrates how much emphasis firms put on appropriating its existing businesses to extract profits, over exploring new opportunities to innovate and create value for consumers. Under the context of this paper, I assume fixing the problem and exploring opportunities for privacy protective businesses to be represented by increase in R&D expenses; I assume interacting with consumers to alleviate consumer concerns and repair reputation in the short-term by advertising expenses. If my hypothesis for the main effect holds (**H1**), a firm will put its emphasis to creating values by exploring new opportunities that would protect privacy over communicating with the consumers after a data breach, decreasing $\mathrm{SE_{it}}$.

I note that expenses related to specific responses, such as insurance payments, could to be lumped into SG&A. It is also possible that a firm categorizes the cost as R&D; in such cases, I interpret that as firm's perspective of the cybersecurity costs as part of their product and service development, as a part of value creation.

3.3 Independent Variables

Data breach. Data breach incident is the main independent variable I investigate. I use a binary variable of whether the firm had a data breach incident in each. While this is straightforward and simple, it may not be sufficient to capture the vastly dissimilar nature of data breach incidents. To account for such differences and test **H8**, I adjust the measure firstly by introducing severity of the breach using how salient the breach was to the consumers, and secondly by narrowing the classification of data breach.

Media coverage: Crises are often notified to the consumers through news media. Increased media coverage signals the severity of the incidents and leads to increased salience of the incidents to the public. This is crucial because consumers can rarely specify the responsible parties when they experience privacy harms, such as identity thefts. Out of all the products and services one uses online and firms they interact with, it is impossible to trace who is actually responsible for their loss. With increased salience of an incident from a firm, consumers are more likely to attribute their fear of loss and damages towards the firm. Therefore, firms will be motivated to explore for additional opportunities other than what they currently have to create values. Their existing values might already have been damaged by the stronger negative sentiment, so the impact of data breach on their emphasis on exploring future opportunities will be intensified. I collect data on media coverage by taking the number of news articles on Factiva that mentions the firm's data breach within one year since the disclosure of the incident.

Data breach characteristics: To further differentiate different types of data breach, I examine whether the firm in the breach event will be viewed as a victim, which will cause mild reputational threat, or it will be perceived to be responsible for the attack,

which will pose more severe reputational threat. Coombs (2007) identifies three types of crises with varying reputational threats, first being victim cluster, then accidental cluster, and finally preventable cluster. If a firm determines that a security incident would cause a severe reputational threat, its strategic response will be more significantly affected than that of a mild threat. In assessing the degree of firm's responsibility in each incident, I categorize breaches hacked by an outsider, malware, or unintended disclosure from internal personnel as the types of breach that have high reputational threat. In these cases, firms are responsible for either their lack of security in their system or control of their employees, so they are less victimized. On the other hand, I categorize other breaches that firms have less control over, such as those involving malicious insider, physical theft, or loss, as the types of breach with mild reputational threat. I incorporate both broad definition of data breach regardless of the extent of firms' responsibility and narrow definition of data breach that would cause high reputational threat and compare how firms' responses differ.

3.4 Moderators

Firm-level moderators. *Firm size* is measured by taking the log of the total number of employees at the firm, collected from Compustat. *Marketing insight* within each firm is identified using Execucomp database, following previous literature (Kashmiri, Nicol, and Hsu 2017; Wies and Moorman 2015). Execucomp releases top five executive officers within a company each year, so I identify firms with a top executive in charge of sales, marketing, brand, or customers as firms with marketing resources in its top management. To identify firms with high *brand value*, I code firms who made into Interbrand's list of top 100 brands each year as top brand firms. Interbrand determines

brand values based on firms' financial performances, brand's role in purchase decisions, and its competitive strength.

Industry-level moderators. *Prevalence of data breach in the industry* is measured by the number of data breach incidents experienced by the firms in the industry that the target firm operates in. Industry is defined using first two digits of NAICS code. *Market concentratio*n is measured as a Herfindahl-Hirschman Index (HHI) which is frequently accepted in marketing and economics literature. Following Jindal and McAlister (2015), *market turbulence* is calculated using market sales as the standard error of the estimated sales growth.

3.5 Control Variables

Firm characteristics: I further control for other firm-specific characteristics that vary over time that could affect its strategic emphases. For instance, I include market scrutiny measured by the number of analysts following the firm in that year, released by Institutional Brokers' Estimate System (Moorman et al. 2012). The firms' financial performances may affect their decisions in spending, such as financial circumstances measured by return on assets, financial leverage, and capital intensity, following previous literature (Lim, Tuli, and Grewal 2020; Mizik 2010). Lastly, I include variables that would affect firms' likeliness to spend on IT technology, such as operational risk (Huang and Wang 2021) and the presence of an IT director.

4. Model

4.1 Model Specification

To identify the impact of data breach on strategic emphasis, I use staggered difference-in-differences (DID) where treated units are the firms that ever experienced a data breach with treatment timing varying over time, and control units are all other firms. I compare how firms exhibit different strategic emphasis in years with and without data breach. This model assumes that data breach will have an impact on the firms' decision in that year that data breach occurred.

Since the data on breach starts in 2005, I am assuming that there were no data breach prior to that year by construction which may bring concerns for left truncation bias. I justify this decision in two ways. First, various sources show that there were very few data breaches prior to 2005 compared to post 2005. In addition Privacy Rights Clearinghouse, Identity Theft Resource Center reports annual number of data breaches starting 2005[6]; Wikipedia keeps track of data breach incidents involving more than 30,000 records, and the list starts in 2004 (with one incident at a Japanese firm)[7]. In addition to the small volume of incidents, data breach posed less of a strategic concern to the firms prior to 2005. California was the only state in the country that had data breach notification laws prior to 2005 (Perkins Cole 2021). Then, in 2005, 10 states introduced the notification laws, signifying the rapid adoption of a measure to notify consumers with a data breach. In addition to the data breach notification laws, California enacted "California Online Privacy Protection Act" which mandated privacy policies, and further

[6] ITRC 2020 Data Breach Report, page 10
[7] https://en.wikipedia.org/wiki/List_of_data_breaches

"Shine the Light Act" which required firms to disclose how they share users' personal information when consumers requested. Without such laws, firms were not obligated to inform their consumers with data breach, and the cost of data breach had been significantly lower. Therefore, even if a firm had a data breach prior to 2005, it would have had minimal impact on firms' decision making.

For the analyses, I consider firms' spending on creating and appropriating values for the public firms in the period of 2004 to 2014. Let *i* indicate firm, and *t* indicate year. Then, for each firm-year, I have a specification that looks like the following:

$$
\begin{aligned}
SE_{it} = \ & \alpha_{0,i} + \alpha_{1,t} + \theta DB_{it} \\
& + DB_{it} \\
& \times (\beta_1 Size_{it} + \beta_2 Mkt_{it} + \beta_3 TopBrand_{it} + \beta_4 IndustryDB_{it} + \beta_5 HHI_{it} \\
& + \beta_6 MTurb_{it}) + \boldsymbol{\gamma} X_{it} + \epsilon_{it}
\end{aligned}
$$

The term DB_{it} equals 1 if firm *i* experiences a data breach in year *t*, and 0 otherwise. I try two different definitions of a "data breach": first includes all types of data breach, regardless of the extent of firm's liability in the incident, and second only looks at those that its business is more accountable for the breach. Because I am interested in firms' immediate response after data breach, I examine only the year of data breach. While I do not expect the strategic adjustment to have permanent impact, firms' decisions on strategic emphasis might not return to their original level prior to the incident. Therefore, for treatment years, I only keep the year of first breach for the post-treatment period.

The terms $\alpha_{0,i}$ and $\alpha_{1,t}$ are firm fixed effects and time fixed effects, respectively; $Size_{it}$ is the logged number of employees at firm *i* in year *t*; Mkt_{it} is 1 if firm *i* has a marketing leader in its top management, 0 otherwise; $TopBrand_{it}$ equals 1 if firm *i* is included in Interbrand's global top 100 brands list in year *t*, 0 otherwise; $IndustryDB_{it}$ is the number of data breach incidents firm *i*'s industry experiences in year *t*; HHI_{it} is the market's HHI in year *t*; $MTurb_{it}$ is market turbulence measure calculated using the variance of regression coefficients of the total sales of the industry that firm *i* operates in; and X_{it} is the set of control variables. While I try to capture and account for industry characteristics and add firm fixed effects, errors (ϵ_{it}) are likely correlated within industries. In estimating the model, I cluster errors by industries using vce option in STATA.

Then, I account for the different severity of the incidents using the salience. Specification mainly stays the same, except that for DB_{it}, I use a salience variable instead of the binary indicator, denoted as DB_{it}^{c} below. 14 of the total 70 incidents have 0 coverage with a median 11.

$$\begin{aligned} SE_{it} = \ & \alpha_{0,i} + \alpha_{1,t} + \theta DB_{it}^{c} \\ & + DB_{it}^{c} \\ & \times (\beta_1 Size_{it} + \beta_2 MktEx_{it} + \beta_3 TopBrand_{it} + \beta_4 IndustryDB_{it} \\ & + \beta_5 MConc_{it} + \beta_6 MTurb_{it}) + \boldsymbol{\gamma} X_{it} + \epsilon_{it} \end{aligned}$$

4.2 Parallel Trends Assumption

A challenge with this model comes from the main DID assumption necessary for its internal validity. For DID estimator to be valid, parallel trend assumptions need to hold: if not for the treatment, difference between the treatment and control group would have been constant over time.

Testing for parallel trends assumption is often done by visualizing the data. In the case of data breach, I cannot simply compare time trend between pre-treatment and post-treatment because treatment timing differs for all firms. It is not clear which years should be compared, especially since control firms never received the treatment (experienced data breach) in the sample period. Instead, I use a linear regression for time trend differences between the groups, controlling for several firm characteristics that could affect the dependent variable. Results shown in **Table 3** suggest that there was a statistically significant change in strategic emphasis for the post-treatment periods of the treatment groups. The year of data breach has a significant negative coefficient, while all years prior to the data breach hold no significance.

Table 3: Parallel Trends Assumption Test

VARIABLES	Data Breach
F4.Data Breach	0.0034
	(0.0056)
F3.Data Breach	-0.0043
	(0.0055)
F2.Data Breach	-0.0052
	(0.0053)
F1.Data Breach	-0.0087
	(0.0054)
Data Breach	-0.014**
	(0.0055)
Number of Analysts Following	0.00083***
	(0.00016)
Return on Assets	0.080***
	(0.0042)
Financial Leverage	0.0052
	(0.0037)
Capital Intensity	-0.045***
	(0.010)
Operational Risk	0.00065
	(0.00053)
IT Executive	-0.0034*
	(0.0018)
Constant	-0.026***
	(0.0026)
Observations	6,859
Adjusted R-squared	0.843

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

5. Results

I first present some descriptive statistics of the data and model-free evidence of potential impact of data breach on strategic emphasis. Then, I present the main results.

5.1 Descriptive Statistics

Table 4 shows summary statistics of the variables used in the model. I have 879 firms reporting for 7.85 years on average in the data for the span of 11 years. About 8% of those firms experienced data breach incident, where almost half of them are those that the firm was not a victim, holding responsibility in the incidents. Data breach incidents are positively correlated with firms that are bigger in size which is consistent with previous literature (Huang and Wang 2021), as well as those with more brand equity. In terms of coverage, the number of articles that mention data breach are higher if the firm in the breach was not a victim and perceived to be more responsible.

Table 4: Summary Statistics

	(1)	(2)	(3)	(4)	(5)
VARIABLES	N	mean	sd	min	max
Number of Employees	6,901	17.6	54.6	0	1,900
Market Turbulence	6,901	0.0032	0.0019	0.00033	0.011
Market Concentration	6,901	522	580	112	8,627
Brand Equity	6,901	0.031	0.17	0	1
Number of Analysts Following	6,901	8.40	7.88	0	47.1
Marketing Insights	6,901	0.30	0.46	0	1
IT Executive	6,901	0.14	0.35	0	1
Operational Risk	6,901	0.069	1.10	0.0016	64.4
Return on Assets	6,901	0.040	0.15	-3.93	0.87
Financial Leverage	6,901	0.17	0.25	0	6.90
Capital Intensity	6,901	0.20	0.17	0	0.94
Data Breach Indicator	6,901	0.010	0.10	0	1
Industry Data Breach Prevalence	6,901	2.73	2.84	0	15

5.2 Regression Results

The results from the regressions are presented in **Table 5** and **Table 6**. As discussed in 4.1, differences in data breach are accounted for using salience measured by coverage (column (2) and (4)) as well as narrower definition of data breach that is more closely related to the firms' business.

I first run regressions of strategic emphasis on data breach along with control variables, without including interactions with firm and industry characteristics that determine their resources which I believe moderate the main effect (**Table 5**). Results show that there is no overall impact of data breach on strategic emphasis between advertising and R&D when I do not account for firms' internal and external resources and their respective strategies depending on those resources. I also note that four operationalizations of data breach across salience and the firm's involvement in the incident do not exhibit much difference in these models without interaction terms.

Table 5: Regression Results without Interactions

VARIABLES	(1) All Data Breach Binary Indicator	(2) All Data Breach Coverage	(3) High Firm Liability Binary Indicator	(4) High Firm Liability Coverage
Data Breach	-0.011	-1.5e-06	-0.0070	-5.2e-06
	(0.0075)	(0.000010)	(0.0061)	(0.000011)
Firm Size	-0.0024	-0.0024	-0.0024	-0.0024
	(0.0053)	(0.0053)	(0.0053)	(0.0053)
Marketing Insights	-0.0048	-0.0049	-0.0048	-0.0049
	(0.0031)	(0.0031)	(0.0031)	(0.0031)
Brand Equity	0.012	0.012	0.012	0.012
	(0.0093)	(0.0089)	(0.0089)	(0.0089)
Industry Data Breach Prevalence	-0.00038	-0.00043	-0.00041	-0.00043
	(0.00044)	(0.00043)	(0.00043)	(0.00043)
Market Concentration	1.6e-07	3.1e-07	3.2e-07	3.1e-07
	(1.9e-06)	(1.9e-06)	(1.9e-06)	(1.9e-06)
Market Turbulence	0.14	0.13	0.13	0.13
	(0.76)	(0.77)	(0.77)	(0.77)
Number of Analysts Following	0.00086***	0.00084***	0.00085***	0.00085***
	(0.00025)	(0.00024)	(0.00024)	(0.00024)
Return on Assets	0.081***	0.081***	0.081***	0.081***
	(0.017)	(0.017)	(0.017)	(0.017)
Financial Leverage	0.0051	0.0049	0.0050	0.0049
	(0.0082)	(0.0082)	(0.0082)	(0.0082)
Capital Intensity	-0.043	-0.043*	-0.043*	-0.043*
	(0.026)	(0.026)	(0.026)	(0.026)
Operational Risk	0.00066***	0.00066***	0.00066***	0.00066***
	(0.00022)	(0.00022)	(0.00022)	(0.00022)
IT Executive	-0.0035	-0.0034	-0.0035	-0.0034
	(0.0029)	(0.0029)	(0.0029)	(0.0029)
Constant	-0.022**	-0.022**	-0.022**	-0.022**
	(0.0086)	(0.0086)	(0.0086)	(0.0086)
Observations	6,859	6,859	6,859	6,859
Adjusted R-squared	0.843	0.843	0.843	0.843

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 6 illustrates a different picture. There is an overall significant negative impact of data breach on strategic emphasis advertising over R&D, both when I use the

binary indicator for data breach and the salience measure, and also both when I use broad and narrow categorization of data breach. In other words, firms on average invest in fixing the problem and creating values for the customers when they experience security threats (**H1**). With a data breach, percentage of the difference in R&D and advertising relative to total assets declines by 5 percentage points (column (1)); if the breach happens to be related to the business operations rather than less controllable mishaps, the discrepancy goes up to 6.7 percentage points (column (3)). I also find that the statistical significance of the impact of data breach on strategic emphasis increases when the salience of the incidents is considered.

Table 6: Regression Results with Interaction Terms

VARIABLES	(1) All Data Breach Binary Indicator	(2) All Data Breach Coverage	(3) High Firm Liability Binary Indicator	(4) High Firm Liability Coverage
Data Breach	-0.053**	-0.00048***	-0.067**	-0.00039***
	(0.022)	(0.000099)	(0.033)	(0.00010)
DB X Firm Size	0.014**	0.000067***	0.0055*	0.000049***
	(0.0058)	(0.000012)	(0.0029)	(0.000011)
DB X Marketing Insights	-0.016	0.000099***	-0.016	0.000058***
	(0.011)	(0.000026)	(0.010)	(0.000021)
DB X Brand Equity	-0.0073	-0.000073**	-0.0041	-0.000072**
	(0.0080)	(0.000030)	(0.0087)	(0.000032)
DB X Industry DB Prevalence	0.0041**	0.000031***	0.0059*	0.000029***
	(0.0018)	(6.5e-06)	(0.0032)	(7.7e-06)
DB X Market Concentration	1.6e-06	9.4e-08*	0.000021*	7.8e-08
	(3.9e-06)	(5.4e-08)	(0.000012)	(5.1e-08)
DB X Market Turbulence	-5.75	0.00083	2.39	0.0068
	(3.63)	(0.021)	(3.61)	(0.022)
Firm Size	-0.0025	-0.0024	-0.0024	-0.0024
	(0.0053)	(0.0053)	(0.0053)	(0.0053)
Marketing Insights	-0.0048	-0.0049	-0.0048	-0.0049
	(0.0031)	(0.0031)	(0.0031)	(0.0031)
Brand Equity	0.013	0.012	0.012	0.012
	(0.0090)	(0.0084)	(0.0089)	(0.0088)
Industry Data Breach Prevalence	-0.00042	-0.00044	-0.00043	-0.00043
	(0.00044)	(0.00043)	(0.00044)	(0.00043)
Market Concentration	6.0e-07	3.6e-07	3.8e-07	3.4e-07
	(1.9e-06)	(1.9e-06)	(1.9e-06)	(1.9e-06)
Market Turbulence	0.13	0.13	0.11	0.14
	(0.77)	(0.77)	(0.77)	(0.77)
Number of Analysts Following	0.00086***	0.00086***	0.00086***	0.00086***
	(0.00024)	(0.00025)	(0.00024)	(0.00025)
Return on Assets	0.081***	0.081***	0.081***	0.081***
	(0.017)	(0.017)	(0.017)	(0.017)
Financial Leverage	0.0056	0.0050	0.0055	0.0049
	(0.0082)	(0.0082)	(0.0083)	(0.0082)
Capital Intensity	-0.044*	-0.043*	-0.043*	-0.043*
	(0.026)	(0.026)	(0.026)	(0.026)
Operational Risk	0.00066***	0.00066***	0.00066***	0.00066***
	(0.00022)	(0.00022)	(0.00022)	(0.00022)
IT Executive	-0.0036	-0.0034	-0.0035	-0.0034
	(0.0030)	(0.0029)	(0.0029)	(0.0029)
Constant	-0.022**	-0.022**	-0.022**	-0.022**
	(0.0086)	(0.0086)	(0.0086)	(0.0086)
Observations	6,859	6,859	6,859	6,859
Adjusted R-squared	0.844	0.843	0.843	0.843

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

I see overall firm's internal resources moderating the impact of data breach on firms' responses. While firm size itself does not explain firms' strategic emphasis between value creation and appropriation, it positively affects the firm's emphasis on value appropriation when they experience a data breach. This suggests that big firms are less likely to make immediate adjustments to their business strategies and more likely to spend on marketing, supporting my hypothesis (**H2**). Moderating effect of firm size attenuates slightly in terms of magnitude when I consider situations where firms are more responsible. Similarly, firms with marketing insights in their management team are more likely to emphasize interacting with consumers and rebuilding reputation, consistent with the hypothesis (**H3**). It is interesting to note that the moderating power of marketing insights is significant only when the incidents are salient to the consumers. Next, brand equity encourages firms to create values for the customers rather than communicating with them (**H4**), also when the incidents are salient. This suggests that brand equity does not influence firms in responding to data breach when it is not well covered by the press.

I see less evidence of firms' external resources from its competitors. Data breach prevalence in the industry they operate in is the only industry resources that is statistically significant in moderating firms' responses. As hypothesized, firms in industries where data breach is more common put more emphasis on communicating with their consumers than to address the problem (**H5**). I still lack statistical evidence of market concentration and market turbulence moderating firm responses to data breach.

Lastly, when I compare across different variations of data breach across salience and classification (**H8**), I see the significance becoming more significant when we account for the salience of the incident. However, when we consider a subset of data

breach incidents that firms are more responsible for, we see the moderating effects are relatively small and less significant. This may be due to our lack of information about the data breach type, and further investigation may be required to better account for the firm accountability in the incidents.

6. Robustness Checks

6.1 Placebo Test

To further test for false positive effects, I implement placebo tests. First, I choose fake treatment year for the firms in treated group to be 2 years prior to the breach.[8] Placebo results in **Table 7** show that the effects are nonexistent compared to what I saw in the main model presented in **Table 6**. This demonstrates the robustness of the results.

[8] I do not use 1 year prior to the breach because sometimes firms report their incident few weeks or months after they find out about the breach; I do not use 3 or more year prior to the breach because it leads to too much data loss.

Table 7: Placebo Tests

VARIABLES	(1) All Data Breach Binary Indicator	(2) All Data Breach Coverage	(3) High Firm Liability Binary Indicator	(4) High Firm Liability Coverage
Data Breach	0.0064	0.000036	0.0025	-0.0038
	(0.0069)	(0.00011)	(0.0076)	(0.014)
DB X Firm Size	-0.000060	-0.000018	0.000035	0.0010
	(0.0013)	(0.000021)	(0.0015)	(0.0031)
DB X Marketing Insights	-0.0048	-0.000041**	-0.00072	
	(0.0052)	(0.000019)	(0.0082)	
DB X Brand Equity	0.0025	0.000041*	0.0059	
	(0.0043)	(0.000024)	(0.0066)	
DB X Industry DB Prevalence	0.0012	-7.1e-06	-0.00034	
	(0.00100)	(4.7e-06)	(0.0011)	
DB X Market Concentration	2.6e-06	9.9e-08*	2.2e-06	
	(2.1e-06)	(5.5e-08)	(2.9e-06)	
DB X Market Turbulence	-4.62***	-0.0054	-1.50	
	(1.23)	(0.0094)	(1.79)	
Firm Size	-0.0010	-0.0010	-0.0010	-0.0010
	(0.0045)	(0.0045)	(0.0045)	(0.0045)
Marketing Insights	-0.0030	-0.0030	-0.0031	-0.0031
	(0.0019)	(0.0019)	(0.0019)	(0.0019)
Brand Equity	0.011	0.014*	0.012	0.012
	(0.0086)	(0.0081)	(0.0091)	(0.0096)
Industry Data Breach Prevalence	-0.000095	-0.000065	-0.000082	-0.000085
	(0.00034)	(0.00034)	(0.00034)	(0.00034)
Market Concentration	8.0e-07	8.4e-07	9.5e-07	9.6e-07
	(1.8e-06)	(1.8e-06)	(1.8e-06)	(1.8e-06)
Market Turbulence	1.17*	1.13*	1.14*	1.12*
	(0.60)	(0.60)	(0.60)	(0.60)
Number of Analysts Following	0.00068***	0.00070***	0.00068***	0.00068***
	(0.00023)	(0.00023)	(0.00023)	(0.00023)
Return on Assets	0.052***	0.052***	0.052***	0.052***
	(0.019)	(0.019)	(0.019)	(0.019)
Financial Leverage	0.0063	0.0066	0.0065	0.0065
	(0.0085)	(0.0085)	(0.0085)	(0.0085)
Capital Intensity	-0.036	-0.036	-0.036	-0.036
	(0.029)	(0.029)	(0.029)	(0.029)
Operational Risk	-0.000032	-0.000034	-0.000032	-0.000033
	(0.00050)	(0.00050)	(0.00050)	(0.00050)
IT Executive	-0.0031	-0.0032	-0.0033	-0.0033
	(0.0034)	(0.0034)	(0.0034)	(0.0034)
Constant	-0.027***	-0.028***	-0.027***	-0.027***
	(0.0077)	(0.0077)	(0.0077)	(0.0077)
Observations	5,279	5,279	5,279	5,279
Adjusted R-squared	0.874	0.874	0.874	0.874

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

6.2 Industries: firms with emphasis in IT

To further account for varying levels of IT focus in each of the firms' businesses, I run the model on a subset of firms where their businesses are closely tied with consumer data, and therefore more sensitive to security incidents. I use Fama-French Industry categorization, and limit the analysis to firms with Fama-French code 5, "Business Equipment – Computers, Software, and Electronic Equipment." This subset includes approximately 30 treated firms and 500 untreated firms. I note that this is different from the data breach prevalence variable, which uses the first two digits of the NAICS code and varies across years.

Results are presented in **Table 8**. It is interesting to see the main effect no longer holds statistical significance, except for the specification where I look at incidents with strong reputational threat as an indicator. In other words, data breach does not affect tech firms' strategic responses between looking for new market opportunities or work on repairing reputation. Two explanations are possible: tech firms may not care much about data breach because it is perceived inevitable, or they are already doing their best to minimize loss from data breach that the actual attack does not shift their strategic emphases. In order to test which of these two conflicting explanations is driving the difference, one would need more in-depth analysis. Unlike the previous results, firms' resource profiles also lost their power to moderate firms' responses to a data breach, and coverage does not significantly change the results.

Table 8: Regression Results, Tech Firms Only

VARIABLES	(1) All Data Breach Binary Indicator	(2) All Data Breach Coverage	(3) High Firm Liability Binary Indicator	(4) High Firm Liability Coverage
Data Breach	-0.15	-0.00020	-0.22**	0.0020
	(0.11)	(0.00049)	(0.094)	(0.0015)
DB X Firm Size	0.022*	0.000096*	0.018***	0.00021
	(0.013)	(0.000048)	(0.0060)	(0.00013)
DB X Marketing Insights	-0.021	0.00014	-0.015	0.00045
	(0.013)	(0.00014)	(0.013)	(0.00036)
DB X Brand Equity	-0.023	-0.00017	-0.031**	-0.00042
	(0.017)	(0.00013)	(0.013)	(0.00029)
DB X Industry DB Prevalence	0.013	0.000013	0.019**	-0.00015
	(0.010)	(0.000045)	(0.0081)	(0.00014)
DB X Market Concentration	0.000017	-1.5e-07	8.6e-06	-2.0e-06**
	(0.000040)	(3.4e-07)	(0.000073)	(9.0e-07)
DB X Market Turbulence	0.67	-0.037	17.7*	-0.30
	(8.00)	(0.057)	(10.4)	(0.19)
Firm Size	0.019***	0.019***	0.019***	0.019***
	(0.0057)	(0.0058)	(0.0058)	(0.0058)
Marketing Insights	-0.0035	-0.0039	-0.0038	-0.0038
	(0.0029)	(0.0033)	(0.0033)	(0.0033)
Brand Equity	0.044	0.041	0.041	0.042*
	(0.027)	(0.026)	(0.026)	(0.025)
Industry Data Breach Prevalence	-0.00037	-0.00036	-0.00035	-0.00036
	(0.00042)	(0.00041)	(0.00042)	(0.00041)
Market Concentration	0.000041**	0.000043**	0.000042**	0.000044***
	(0.000016)	(0.000016)	(0.000017)	(0.000016)
Market Turbulence	-1.75**	-1.95**	-1.97**	-1.96**
	(0.84)	(0.93)	(0.93)	(0.93)
Number of Analysts Following	0.00096***	0.00099***	0.00097***	0.00098***
	(0.00027)	(0.00028)	(0.00028)	(0.00028)
Return on Assets	0.090***	0.090***	0.090***	0.090***
	(0.015)	(0.015)	(0.015)	(0.015)
Financial Leverage	0.017	0.016	0.016	0.016
	(0.019)	(0.019)	(0.019)	(0.019)
Capital Intensity	-0.19**	-0.19**	-0.19**	-0.19**
	(0.075)	(0.074)	(0.075)	(0.074)
Operational Risk	0.00013	0.00011	0.00011	0.00011
	(0.00014)	(0.00014)	(0.00015)	(0.00015)
IT Executive	-0.0083	-0.0077	-0.0077	-0.0077
	(0.0050)	(0.0050)	(0.0050)	(0.0050)
Constant	-0.094***	-0.095***	-0.094***	-0.095***
	(0.012)	(0.012)	(0.012)	(0.012)
Observations	2,217	2,217	2,217	2,217
Adjusted R-squared	0.803	0.799	0.799	0.799

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

7. Conclusion

With a growing scrutiny around firms' collection and use of consumer data, both from the regulators and the public, firms are pressured to take privacy concerns into account in operating their businesses. Consequently firms face the growing demand for consumer privacy and protect them by architecture. In this paper, I present empirical evidence that these incidents encourage firms to build new products or services to make their businesses more robust to such attacks. It might look like if data breach does not affect firms' strategic responses (**Table 5)**, I find that firms invest in exploring new opportunities for businesses after a security incident when firm resources are considered (**Table 6**). I also report quite a variation among the firms depending on their resources, especially those they own internally. Namely, big firms with emphasis on marketing insights in an industry commonly exposed to security incidents will have stronger emphasis on communicating with their customers, whereas firms with strong brands will be likely to put efforts to fix their problems and innovate. Without considering firms' resource profiles, however, it will be easy to overlook how data breach affects their strategic responses.

7.1 Implications

This research was motivated by the aspiration to contribute to our understanding of how the businesses are responding and transforming with the growing privacy concerns in the society. Findings from the paper suggest that firms respond to the increasing scrutiny over security incidents and how firms handle data. In addition to firms' regulatory compliance and increasing self-regulatory measures such as third-party cookie ban, firms make strategic adjustments in response to privacy concerns. Even

though this paper only looks at firms' reactive responses rather than proactive measures, firms shift their strategic emphases to better incorporate the concerns.

However, the magnitude of the impact is pretty small. Firms' business strategies on average are not much affected by data breach. This could be due to several reasons. Firms might be adjusting different components of the spending. For instance, their emphasis between value appropriation and creation might not have changed, but the focus within looking for future opportunities might have changed. They might be reallocating their resources to focus on privacy sensitive products and less on different opportunities, but such reallocation within the R&D will not be captured in the model. Another possibility is that firms do not take data breach as a significant concern, unlike what they claim. Previous literature suggests that data breach involving sensitive information, such as personally identifiable information (Labrecque et al. 2021) or financial information (Kamiya et al. 2021; Romanosky, Hoffman, and Acquisti 2014), has a more damaging impact on the involved firms. While I attempt to account for possible variation in impact with salience and firm responsibility, additional investigation at the firms' responses on a granular level of information type would be necessary to draw more definite conclusions, such as limiting the analyses to incidents involving sensitive information and see how that affects the firms' decisions.

7.2 Limitations

Although this paper is among the few in marketing to study how firms respond to data breach, I would like to conclude with limitations and potentially additional research that could follow. First, I look at the broad expense categories of R&D and advertising. Firms may be increasing their budget for new opportunities through R&D, but I do not

know how they are spending the money. They could be trying to develop a trickier way to collect consumer data that is more detrimental for the consumers, or they could be venturing out to new avenues of business. More in-depth investigation, either qualitative or quantitative, on how firms are specifically changing their businesses would be necessary to better assess the impact of data breach on the firms.

Also, the sample is restricted to public firms because I look at advertising and R&D expenses to operationalize firms' emphases on value creation and appropriation. However, data breach incidents also involve other various entities, including private firms, non-profit firms, and hospitals. For a better understanding of how firms respond to data breach, it would be valuable to utilize different measures for strategic emphasis to include non-public firms and see how they are affected by the incidents. In addition, I rely on reported expenses restrict the analyses on an annual level. While decisions on strategic emphases may be planned on a long term and annual analyses may be appropriate, firms' responses to data breach might have more temporal impact that is not captured from strategic emphases. Other measures to investigate firms' responses may be helpful for a more complete picture of how firms regard consumer privacy. Few examples that would show constructive improvements include change in security spending, amount of data collection or reliance on consumer data, and increase in privacy features; those for transferring control to consumers include change in privacy policies and consent requirements.

References

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. 2006. “Is There a Cost to Privacy Breaches? An Event Study.” *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*: 1563–80.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. “The Economics of Privacy.” *Journal of Economic Literature* 54(2): 442–92.

Anderson, Ross et al. 2019. “Measuring the Changing Cost of Cybercrime.” *Workshop on the Economics of Information Security (WEIS)*: 1–32. http://orca.cf.ac.uk/id/eprint/122684.

Athey, Susan, Christian Catalini, and Catherine Tucker. 2017. “The Digital Privacy Paradox: Small Money, Small Costs, Small Talk.” *NBER*.

Bisogni, Fabio. 2015. *Data Breaches and the Dilemmas in Notifying Customers*.

Boyd, D. Eric, Rajesh K. Chandy, and Marcus Cunha. 2010. “When Do Chief Marketing Officers Affect Firm Value? A Customer Power Explanation.” *Journal of Marketing Research* 47(6): 1162–76.

Campbell, Katherine, Lawrence A Gordon, Martin P Loeb, and Lei Zhou. 2003. “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence Form the Stock Market.” *Journal of Computer Security* 11(11): 431–48. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.7735&rep=rep1&type=pdf%0Ahttps://web-a-ebscohost-com.libproxy.smu.edu.sg/ehost/pdfviewer/pdfviewer?vid=1&sid=e13ea18f-2e81-45a7-b39f-3dea6201f87c%40sdc-v-sessmgr06.

Challagalla, Goutam, Brian R. Murtha, and Bernard Jaworski. 2014. “Marketing Doctrine: A Principles-Based Approach to Guiding Marketing Decision Making in Firms.” *Journal of Marketing* 78(4): 4–20.

Chandy, Rajesh K, and Gerard J Tellis. 2000. “The Incumbent’s Curse? Incumbency, Size, and Radical Product Innovation.” *Jounal of Marketing* 64(7): 1–17.

Chen, Long, Yadong Huang, Shumiao Ouyang, and Wei Xiong. 2021. “The Data Privacy Paradox and Digital Demand.” (March).

Citron, Danielle Keats, and Daniel J. Solove. 2021. “Privacy Harms.” *SSRN Electronic Journal* (20).

Cole, Lauren Lyons. 2017. “After the Equifax Breach , Consumers Were Advised to Freeze Their Credit — but Almost No One Did It.” *Business Insider*: 1–2.

Coombs, W. Timothy. 2007. “Protecting Organization Reputations During a Crisis: The

Development and Application of Situational Crisis Communication Theory." *Corporate Reputation Review* 10(3): 163–76.

Donaldson, Lex. 2001. *The Contingency Theory of Organizations*. Sage.

Eilert, Meike, Satish Jayachandran, Kartik Kalaignanam, and Tracey A. Swartz. 2017. "Does It Pay to Recall Your Product Early? An Empirical Investigation in the Automobile Industry." *Journal of Marketing* 81(3): 111–29.

Foerderer, Jens, and Sebastian W. Schuetz. 2022. "Data Breach Announcements and Stock Market Reactions: A Matter of Timing?" *Management Science* (March).

Gay, Sebastien. 2017. "Strategic News Bundling and Privacy Breach Disclosures." *Journal of Cybersecurity* 3(2): 91–108.

Germann, Frank, Peter Ebbes, and Rajdeep Grewal. 2015. "The Chief Marketing Officer Matters!" *Journal of Marketing* 79(3): 1–22.

Gwebu, Kholekile L., Jing Wang, and Li Wang. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management." *Journal of Management Information Systems* 35(2): 683–714. https://doi.org/10.1080/07421222.2018.1451962.

Han, Kyuhong, Vikas Mittal, and Yan Zhang. 2017. "Relative Strategic Emphasis and Firm-Idiosyncratic Risk: The Moderating Role of Relative Performance and Demand Instability." *Journal of Marketing* 81(4): 25–44.

Hsu, Po-Hsuan, Wei-Chuan Kao, and Yanzhi Wang. 2021. *Cybersecurity and Brand Capital*.

Huang, Henry He, and Chong Wang. 2021. "Do Banks Price Firms' Data Breaches?" *The Accounting Review* 96(3): 261–86.

Janakiraman, Ramkumar, Joon Ho Lim, and Rishika Rishika. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer." *Journal of Marketing* 82(2): 85–105.

Jindal, Niket, and Leigh McAlister. 2015. "The Impacts of Advertising Assets and R&D Assets on Reducing Bankruptcy Risk." *Marketing Science* 34(4): 555–72.

Johnson, Garrett, and Scott K. Shriver. 2020. "Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR." *SSRN Electronic Journal*.

Josephson, Brett W., Jean L. Johnson, and Babu John Mariadoss. 2016. "Strategic Marketing Ambidexterity: Antecedents and Financial Consequences." *Journal of the Academy of Marketing Science* 44(4): 539–54. http://dx.doi.org/10.1007/s11747-015-0438-5.

Kamiya, Shinichi et al. 2021. “Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms.” *Journal of Financial Economics* 139(3): 719–49. https://doi.org/10.1016/j.jfineco.2019.05.019.

Kashmiri, Saim, Cameron Duncan Nicol, and Liwu Hsu. 2017. “Birds of a Feather: Intra-Industry Spillover of the Target Customer Data Breach and the Shielding Role of IT, Marketing, and CSR.” *Journal of the Academy of Marketing Science* 45(2): 208–28.

Labrecque, Lauren I, Ereni Markos, Kunal Swani, and Priscilla Pe. 2021. “When Data Security Goes Wrong: Examining the Impact of Stress, Social Contract Violation, and Data Type on Consumer Coping Responses Following a Data Breach.” *Journal of Business Research* 135(June): 559–71.

Lane, Kevin. 1991. “Conceptualizing, Measuring, and Managing Customer-Based Brand Equity.” *Working Papers (Faculty) -- Stanford Graduate School of Business*: 46p. http://content.epnet.com/ContentServer.asp?T=P&P=AN&K=13046790&EbscoContent=dGJyMNLe80SeqK84yOvqOLCmr0mep7BSrq64SbKWxWXS&ContentCustomer=dGJyMPGusU6wp7ZIuePfgeyx%2BEu3q64A&D=bth%5Cnpapers3://publication/uuid/A5A4CEB4-6808-45B0-A2C8-1664208133CF.

Lim, Leon Gim, Kapil R. Tuli, and Rajdeep Grewal. 2020. “Customer Satisfaction and Its Impact on the Future Costs of Selling.” *Journal of Marketing* 84(4): 23–44.

Makridis, Christos. 2021. “Do Data Breaches Damage Reputation? Evidence from 45 Companies Between 2002 and 2018.” *SSRN Electronic Journal*: 1–23.

Malhotra, Arvind, and Claudia Malhotra. 2011. “Evaluating Customer Information Breaches as Service Failures: An Event Study Approach.” *Journal of Service Research* 14(1): 44–59.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. 2017. “Data Privacy: Effects on Customer and Firm Performance.” *Journal of Marketing* 81(1): 36–58.

Martin, Kelly D., Brett W. Josephson, Gautham G. Vadakkepatt, and Jean L. Johnson. 2018. “Political Management, Research and Development, and Advertising Capital in the Pharmaceutical Industry: A Good Prognosis?” *Journal of Marketing* 82(3): 87–107.

Mizik, Natalie. 2010. “The Theory and Practice of Myopic Management.” *Journal of Marketing Research* 47(4): 594–611.

Mizik, Natalie, and Robert Jacobson. 2003. “Trading off between Value Creation and Value Appropriation: The Financial Implications of Shifts in Strategic Emphasis.” *Journal of Marketing* 67(January): 63–76.

———. 2007. “Myopic Marketing Management: Evidence of the Phenomenon and Its Long-Term Performance Consequences in the SEO Context.” *Marketing Science* 26(3): 361–79.

Moorman, Christine, Simone Wies, Natalie Mizik, and Fredrika J. Spencer. 2012. "Firm Innovation and the Ratchet Effect among Consumer Packaged Goods Firms." *Marketing Science* 31(6): 934–51.

Romanosky, Sasha, David Hoffman, and Alessandro Acquisti. 2014. "Empirical Analysis of Data Breach Litigation." *Journal of Empirical Legal Studies* 11(1): 74–104.

Rosati, Pierangelo, and Theo Lynn. 2021. "A Dataset for Accounting, Finance and Economics Research on US Data Breaches." *Data in Brief* 35: 106924. https://doi.org/10.1016/j.dib.2021.106924.

Shocker, Allan D., and David A. Aaker. 1993. "Managing Brand Equity." *Journal of Marketing Research* 30(2): 256.

Solove, Daniel J., and Danielle Keats Citron. 2018. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96(4): 737–86.

Swaminathan, Vanitha, Feisal Murshed, and John Hulland. 2008. "Value Creation Following Merger and Acquisition Announcements: The Role of Strategic Emphasis Alignment." *Journal of Marketing Research* 45(1): 33–47.

Teece, David J., Gary Pisano, and Amy Shuen. 1997. "Dynamic Capabilities and Strategic Management." *Strategic Management Journal*.

Turjeman, Dana, and Fred M. Feinberg. 2019. "When the Data Are Out: Measuring Behavioral Changes Following a Data Breach." *SSRN Electronic Journal* (July).

Wies, Simone, Arvid Oskar Ivar Hoffmann, Jaakko Aspara, and Joost M.E. Pennings. 2019. "Can Advertising Investments Counter the Negative Impact of Shareholder Complaints on Firm Value?" *Journal of Marketing* 83(4): 58–80.

Wies, Simone, and Christine Moorman. 2015. "Going Public: How Stock Market Listing Changes Firm Innovation Behavior." *Journal of Marketing Research* 52(5): 694–709.

Zhao, Yi, Ying Zhao, and Kristiaan Helsen. 2011. "Consumer Learning in a Turbulent Market Environment: Modeling Consumer Choice Dynamics after a Product-Harm Crisis." *Journal of Marketing Research* 48(2): 255–67.

Zou, Yixin, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. "You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications." : 1–14.