The Business Value of Engaging in Counter-Breach Initiatives

Taha Havakhor  
Oklahoma State University  
taha.havakhor@okstate.edu

Tianjian Zhang  
Oklahoma State University  
tj.zhang@okstate.edu

Bryan Hammer  
Oklahoma State University  
bryan.hammer@okstate.edu

Abstract

Facing an increasing information security threat, companies react by engaging in various counter-breach initiatives. The business value of such initiatives is under-studied. This paper utilizes an organizational legitimacy view, overlaid by behavioral theory of the firm (BTOF), to examine whether counter-breach initiatives are rewarded by the market, and whether the magnitude of such rewards depends on the institutional environment. Based on a dataset of 3,212 observations from 2005 to 2015, and focusing on counter-breach initiatives that are revealed in public announcements and/or emphasized in annual reports, the results unfold an overall significant positive effect of counter-breach initiatives on Tobin’s q and future return on assets. The findings reveal that this effect is more pronounced for breached firms in low-risk industries and un-breached firms in high-risk industries. This paper contributes to the information security literature by showing the positivity, as well as institutional heterogeneity, of the business value of counter-breach initiatives.

Keywords

Information security; counter-breach initiative; annual report; public announcement; Tobin’s q

Introduction

As information security incidents become more prevalent, firms respond by engaging in counter-breach initiatives, such as investment in intrusion detection technologies, acquiring a successful cybersecurity startup, and changing hiring policies to recruit more engineers with a cybersecurity background. However, the ubiquity of security incidents may numb the investors and cast doubt on the value of such initiatives. On one hand, announcing security measures shows the managerial emphasis on information security, which ultimately protects stakeholders’ value. On the other hand, such announcements may turn into industrial routines to which investors may eventually become unresponsive to (hereafter referred to as the numbing effect). Moreover, counter-breach initiatives are often regarded as inevitable cost elements (Kvochko and Pant 2015), and therefore, their effect on firm profitability is not clear and has not been investigated empirically.

Most studies on economics of information security focus on the market reaction towards security breaches¹ (Campbell et al. 2003; Cavusoglu et al. 2004; Goel and Shawky 2009; Kannan et al. 2007). While knowing the impact of security breaches informs managers of what is at stake when a firm’s security vulnerabilities are exploited, it is also imperative to know the extent to which counter-breach initiatives generate economic rent. Specifically, given the speculation about the numbing effect and skepticism about the nature of counter-breach initiatives as merely cost elements, empirical research in this area can be informing. However, only a limited, although growing, body of research on the value of, and the market reaction to, counter-breach initiatives exists (Chai et al. 2011; Gordon et al. 2010; Wang et al. 2013). To bridge this gap,

¹ A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. Examples include data theft, denial-of-service, malware attacks, etc.
The Business Value of Counter-Breach Initiatives

this study investigates: a) whether engaging in counter-breach initiatives creates business value (RQ1); and b) the conditions under which the value created is greater (RQ2).

Guided by the organizational literature that investigates the business value of similar investments, such as corporate social responsibility investments (McWilliams and Siegel 2001), with a cost-of-doing-business nature but a high impact on customer-valued intangibles, this study adopts a theoretical lens that considers organizational legitimacy as the driving force that makes counter-breach initiatives profitable. In selecting from plausible organizational legitimacy lenses, and considering the numbing effect observation that emphasizes the relative legitimacy of a firm vis-à-vis that of its competitive environment, we adopt the behavioral theory of the firm (BTOF) (Cyert and March 1963; Greve 1998) to investigate the study’s two research questions. BTOF explains the expected actions taken by a firm triggered by a comparison to institutional norms. Therefore, it provides a lens to evaluate the business value of engaging in counter-breach initiatives while considering the institutional patterns of occurrence of those incidents.

In this paper, we study counter-breach initiatives gathered from two sources: those publicly announced through press releases, and those that are emphasized in annual reports by a firm’s executives. Accordingly, a dataset is constructed by tracking related public announcements and investigating organizational annual reports. The economic impacts of engaging in counter-breach initiatives, broadcasted via public announcements and annual reports, are tested in industries with different security breach risk levels in a matched sample of 3,212 firm-year observations, spanning from 2005 to 2015. The results indicate a general positive impact of engaging in counter-breach initiatives both on contemporaneous values of Tobin’s q and later values of return on assets (ROA) across industries with varying risk, although this positive impact is stronger for a firm that either over-performs (i.e., the firm is not affected by a security breach in that year but operates in a high-risk industry) or under-performs its industry (i.e., the firm is affected by a security breach in that year but operates in a low-risk industry).

This paper contributes to the economics of information security by providing evidence supporting the business value and profitability of engaging in counter-breach initiatives. The heterogeneity in the value accrued from counter-breach initiatives in different risk environments unfolds the appropriate firm reactions to security breaches in its institutional environment. For practitioners, this paper will shed light on how market investors evaluate counter-breach initiatives that are broadcasted in public announcements and annual reports. The rest of the article is organized as follows. We review the relevant legitimacy and BTOF literature and develop hypotheses in the next section, followed by data collection and analysis. Finally, we discuss the limitations and implication of the study.

Theoretical Development

Counter-Breach Initiatives and the Business Value

Engaging in counter-breach initiatives has been mostly considered as a mechanism through which a firm protects itself from the fallouts of a security hazard. However, its impact on business value and profitability has remained an empirical question. Counter-breach initiatives are rarely treated as direct factors of production, and instead, are considered as essential costs of doing business in today’s markets. As such, understanding their business value extends beyond the conventional theories of productivity that dominate the business value of IT (BVIT) literature. The existing strategic management literature (McWilliams and Siegel 2001) suggests that gaining organizational legitimacy is an intangible payoff of engaging in initiatives valued by stakeholders of a firm that are otherwise considered cost to the business (e.g., social responsibility initiatives). Organizations are embedded in a web of connections with stakeholders that supply them with financial, trust, and reputational resources (Granovetter 1992). Therefore, actions that increase a firm’s legitimacy among its stakeholders can help a firm increase its economic gains in a market. Hence, a firm may engage in activities that may not directly contribute to the value of its product or service, but are important and valuable to stakeholders. Engaging in such activities signals a firm’s valuing its stakeholders and leads to its enhanced legitimacy.

Specifically, a legitimacy view can illuminate the business value of engaging in counter-breach initiatives. Apart from creating cost-saving rents by mitigating future possible interruptions to the business, a firm

---

2 The security risk of an industry is defined as the relative frequency of security breaches in that industry.
may also appropriate value from counter-breach initiatives through increasing its legitimacy in the eyes of stakeholders. A firm’s valuation in the stock market will be influenced by the legitimacy of the firm because there is a social construction dimension to market values (Rindova et al. 2006; Zajac and Westphal 2004). Since security breaches are expected to negatively impact trust (Acquisti et al. 2006; Cavusoglu et al. 2004) and thereby legitimacy of a firm, engaging in counter-breach initiatives and broadcasting it to the stakeholders may meet economic rewards. A firm may either broadcast its counter-breach initiatives via press releases or use its executives’ direct channels of communication with stakeholders, e.g., annual reports. Based on the tenets of the legitimacy view we expect:

**Hypothesis 1(a):** Announcements made about counter-breach initiatives will be associated with higher business value.

**Hypothesis 1(b):** Emphasizing counter-breach initiatives in annual reports will be associated with higher business value.

**Heterogeneity in the Business Value**

While the broad lens of legitimacy allows hypothesizing about the overall impact of engaging in counter-breach initiatives, a market’s reaction to such initiatives may be stronger in certain conditions. Stock market reactions are affected by the prevailing institutional norms (Zajac and Westphal 2004). Since it is difficult for investors to evaluate the subsequent information security level of a firm as a result of engaging in a counter-breach initiative, they are likely to rely on assessments of a firm’s institutional environment to inform their judgments (Doh et al. 2010). Oftentimes, legitimate firms incur less unsystematic stock market risk than illegitimate firms (Bansal and Clelland 2004). Hence, an organizational legitimacy theory that allows evaluating the counter-breach actions of a firm relative to its institutional environment might best fit understanding the heterogeneity in the business value of counter-breach initiatives. One such theory is the behavioral theory of the firm (BTOF) 3.

BTOF, largely stemming from the seminal work by Cyert and March (1963), explains organizational and strategic changes as a result of a firm’s under- or over-achieving its aspirations (Greve 1998; Park 2007). A socio-economic view in BTOF suggests that aspirations of a firm are adjusted relative to the performance of its competitors in the market. BTOF suggests that when a firm’s performance falls below its aspirations, creating a situation of negative attainment discrepancy, the firm is expected to engage in problemistic search (Miller and Chen 1994). The engagement in problemistic search is intended to return firm performance to acceptable levels. Conversely, when performance is above a firm’s aspiration level (i.e. positive attainment discrepancy), the firm is expected to engage in slack or experimental search (Bourgeois and Singh 1983; Greve 2003; Iyer and Miller 2008; Nohria and Gulati 1996). Finally, firms that perform near their aspiration level are unmotivated to engage in search as performance aspirations are being met and thus are less expected to engage in organizational learning (Cyert and March 1963; Levitt and March 1988). As such, BTOF provides a framework through which the legitimacy of organizational change is assessed by stakeholders: a firm under- or over-performing relative to the performance level of other firms in its environment is expected to engage in organizational initiatives that change the current course. The tenets of BTOF explain organizational choices as legitimizing actions. While a broad body of literature in this area applies the BTOF lens to explain the logic underlying organizational actions, we apply this lens to examine why organizational actions consistent with the predictions of BTOF are rewarded by stakeholders. We believe that this application of the theory is valid as it builds on the assumption that organizational actions consistent with the predictions of BTOF are legitimate, and thereby, engaging in such actions enhances the organizational legitimacy as perceived by stakeholders.

A firm’s engagement in counter-breach initiatives can be understood by tenets of BTOF. A firm affected by a security breach in a low-risk industry, where breaches are rare, is considered under-performing relative to its institutional environment, while a breached firm in a high-risk industry, where breaches happen frequently, is considered performing as expected (Greve 1998). Similarly, an un-breached firm in a low-risk

---

3 Contrary to IT investments that aim to generate revenue (e.g. ERP), a counter-breatch initiative is similar to corporate social responsibility, which is traditionally assumed as an initiative with a cost nature and is known to enhance the business value through increasing the firm’s legitimacy. While traditional BVIT theories (e.g. resource-based view) may be suitable in explaining the profitability of revenue-generating IT investments, both the cost characteristic of counter-breatch initiatives and the consequent market reactions to such initiatives (e.g., “numbing effect”) suggest plausibility of a theory that takes into consideration the social evaluation of organizational choices. BTOF is one such theory.
industry is performing as expected, while an un-breached firm in a high-risk industry is over-performing. Whenever there is a mismatch between a firm’s information security level and its industrial peers, the firm’s engagement in counter-breach initiatives is more legitimized. On one hand, a breached firm in a low risk industry should take the necessary actions to restore its lost trust or lose the competition to rivals that boast a higher security protection. On the other hand, to sustain its rare and valuable position, an un-breached firm in a high-risk industry should capitalize on its strong record and prevent future breaches. Therefore, we expect that:

**Hypothesis 2:** The increase in business value due to announcements about counter-breach initiatives are greater for: (a) breached firms in low-risk industries; and (b) un-breached firms in high-risk industries.

**Hypothesis 3:** The increase in business value as a result of emphasizing counter-breach initiatives in annual reports are greater for: (a) breached firms in low-risk industries; and (b) un-breached firms in high-risk industries.

**Methods**

**Data**

The hypotheses are evaluated based on a dataset about publicly-announced security breaches as well as counter-breach initiatives. For the period of 2005 to 2015, an online search was conducted for public announcements made at all news sources available at Lexis-Nexis, using a set of terms associated with counter-breach initiatives and security breaches, such as: cyber-attack, security breach, phishing, hack, hacking, cyber fraud, denial of service, computer security, and cyber security. News releases from this online search were compiled by two graduate assistants to: a) eliminate duplicate announcements; b) eliminate irrelevant announcements (i.e., announcements that are not about a security breach or counter-breach initiative); and c) categorize the announcements into two broad groups of breaches or counter-breach initiatives. The students’ eliminations of duplicates, irrelevant announcements, and categorizations converged in 98%, 91%, and 87% of instances. In a consecutive round, the disagreements were resolved through revisiting the initial schemes and definitions pertaining to the study. This process yielded 4,871 announcements about security breaches belonging to 3,978 firms and 2,884 announcements about counter-breach initiatives made by 1,673 firms. Since access to financial reports and other organizational information is key to test the study’s hypotheses, from the initial set of announcements about counter-breach initiatives, only those made by publicly-traded firms were retained, yielding 1,606 firm-year observations that belong to 612 unique firms (Sample A). Since focusing solely on firms with a counter-breach announcement can make the study biased, to evaluate the impact of announcing a counter-breach initiative, we adopt a matched sample approach (Bharadwaj 2000; Chae et al. 2014). For each firm-year observation with an announced counter-breach initiative in Sample A, a matching observation with no public announcement about counter-breach initiatives (a publicly-traded firm within 30 percent range of total assets of a focal firm and in the same two-digit SIC code) was added to the sample, extending the Sample A to include 3,212 firm-year observations belonging to 1,481 firms mostly active in retailing, banking, air transportation, insurance, healthcare, and education industries. To estimate the extent of occurrence of security breaches in the industry in which each observation in Sample A is active, from the initial set of announcements about security breaches, only those made by publicly-traded firms and with a two-digit SIC code matching to at least one observation with a public announcement in Sample A in a given year were retained, yielding 2,717 firm-year security breach announcements made by 2,308 firms (Sample B). Utilizing COMPUSTAT, the data from Sample A was then supplemented with various financial and organizational information.

**Measures**

We measure the business value of counter-breach initiatives by evaluating the impact on the firm’s Tobin's q ratio, following Bharadwaj et al. (1999) and Chari et al. (2008). Tobin's q is a forward-looking

---

4 For brevity, we do not include the complete list of search keywords. A complete list is available upon a request sent to the corresponding author.
5 Each of these firm-year observations had only one announcement per year. We did not find any observations where a firm made multiple counter-breach announcements in the same year.
measure of firm value, which is market-oriented, risk adjusted, less sensitive to accounting practices. It is considered appropriate in studies that evaluate the impact of IT-related initiatives (Chari et al. 2008) which may take time to show their impact in other financial measures pertaining to profitability. A Tobin’s $q$ value above one indicates that the long-run equilibrium market value of the firm is greater than the replacement value of its assets, signifying an unmeasured source of value (Bharadwaj et al. 1999). Tobin’s $q$ ratio is calculated as: $q = (\text{Market value of equity} + \text{book value of inventories} + \text{liquidating value of preferred stock} + \text{long-term debt} + \text{net short-term debt})/\text{Total assets}$ (Chung and Pruitt 1994).

To assess a firm’s involvement in counter-breach security initiatives, we utilize two measures: a) a 0/1 dummy variable that is set at 1 if the firm makes a public announcement about a counter-breach initiative (announcement (ANN)); and b) the extent to which a firm verbally emphasizes counter-breach initiatives in its annual reports (i.e., 10-Ks and 10-KSBs; annual reports emphasis (ARE)). To estimate the annual reports emphasis, 3,212 annual reports belonging to each firm-year observation were accessed. Then a lexical search engine was used to highlight paragraphs in the reports that include any of the keywords that were originally used in the Lexis-Nexis search in the study. Then, two graduate students reviewed the highlighted paragraphs to determine if they involve a discussion of how a firm currently engages in, or plans to engage in, counter-breach initiatives. Finally, the natural log of ratio of paragraphs pertaining to counter-breach initiatives to the total number of paragraphs in that year’s annual reports was used as the measure of annual reports emphasis.

We control for year and industry using dummies. We define industry at the two-digit SIC code level to control for several industry-level variables (industry $q$, capital intensity, concentration, and regulation). We also control for several firm-level variables (related diversification, size, assets, R&D expenditure, and advertising expenditure). We measure related diversification using the entropy measure (Robins and Wiersema 1995) used in prior literature (Bharadwaj 2000). We measure firm size as the natural log of the number of employees in thousands. A firm’s total assets reported in COMPUSTAT is used as the measure of assets. The R&D and advertising expenditures were estimated as a ratio of budgetary investments in R&D and advertising, as reported in COMPUSTAT, divided by the firm’s annual revenue.

To control for industry-level variables, we compute industry $q$ as the median of the Tobin’s $q$ ratios of all firms in the industry, industry capital intensity as the median of the capital intensities of the firms in that industry, industry concentration as the Herfindahl index of the market shares of the top four firms in that industry, and regulation as a binary variable, set at one for regulated industries and zero otherwise. Table 1 presents the mean and standard deviation of these variables as well as the listwise correlations among them.

### Estimation

To test the hypotheses, we split sample A into four subsamples based on two criteria: a) whether one or more security breaches have occurred at each firm-year observation in the same year based on information from Sample B; and b) whether the industry (based on two-digit SIC code) in which a focal firm-year observation is active has endured a high or low frequency of security breaches (based on a median split of frequency of breaches happening in each industry in a given year, utilizing information from Sample B). The four sub-samples are: a) firms with one or more security breaches announced while active in an industry with a low frequency of security breaches in a year (ss1); b) firms with one or more security breaches announced while active in an industry with a high frequency of security breaches (ss2); c) firms with no security breaches announced while active in an industry with a low frequency of security breaches (ss3); and d) firms with no security breaches announced while active in an industry with a high frequency of security breaches (ss4). For each sub-sample, the following equation is estimated:

$$q_{it} = B_1 * \text{ANN}_{it} + B_2 * \text{ARE}_{it} + B_3 * \text{diversification}_{it} + B_4 * \text{size}_{it} + B_5 * \text{asset}_{it} + B_6 * \text{R&D}_{it} + B_7 * \text{advertising}_{it} + B_8 * \text{industry}_q_{it} + B_9 * \text{industry}_c_{it} + B_{10} * \text{industry}_n_{it} + B_{11} * \text{regulation}_{it} + \text{YEAR} + \text{INDUSTRY} + \epsilon_{it}$$

where subscripts $i$ and $t$ denote the firm $i$ in year $t$. $\epsilon_{it}$ is the error term and $c_i$ is the firm-specific time-invariant unobserved heterogeneity term.
Before estimating the models, all variables are standardized. Considering the panel structure of the data, a Hausman test is run in order to select the appropriate random-effects or fixed-effects model and remove the effect of the time-invariant unobserved heterogeneity term (i.e., $c_t$). The results of this test fail to reject the null hypothesis that the firm-level effects are adequately modeled by a random-effects model ($\chi^2(28) = 1.35, p > 0.10$). Next, we conduct likelihood ratio tests to understand the panel-specific heteroskedasticity and the panel-specific auto-correlation structure of the data. The results of the likelihood ratio tests indicate the presence of panel-specific heteroskedasticity ($LR \chi^2(28) = 414.14, p < 0.001$), as well as panel-specific auto-correlation ($PSAR1; LR \chi^2(28) = 407.79, p < 0.001$). Accordingly, a feasible Generalized Least Square (GLS) regression with corrections for $PSAR1$ autocorrelation and panel-specific heteroskedasticity is used to estimate the coefficients of the proposed models.

### Results

Table 2 presents the results of the estimation for each subsample (ss1-ss4). The coefficients of both ANN and ARE variables are positive and significant in all cases (supporting H1a and H1b), with the exception of the coefficient of ARE in ss2, where the firm engaging in a counter-breach initiative has both been impacted by a security breach in that year and operates in an industry with a high frequency of security breaches happening. The results suggest that the highest positive effect sizes associated with ANN and ARE are observable in ss1 and ss4, where under-performing or over-performing firms engage in counter-breach initiatives. Table 3 shows the results of a series of $t$-tests that compare the effect sizes of ss1 and ss4 with other sub-samples for both ANN and ARE estimates. The effect size of ANN variable in ss1 is higher than that of all other sub-samples (providing support to H2a), whereas the effect size of ANN variable in ss4 is higher than that of ss3, but not ss2's (providing support to H2b). Moreover, the effect size of ARE variable in ss1 is higher than that of ss2 (providing support to H3a), whereas the effect size of ARE variable in ss4 is higher than that of ss3 (providing support to H3b). Taken together, the results suggest that while engaging in counter-breach initiatives generally increase a firm’s Tobin’s $q$, the impact is stronger for firms that have under or over-performed relative to other firms in their industry.

### Table 1. Correlation Matrix

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>1.09</td>
<td>0.50</td>
<td>-6.06</td>
<td>2.98</td>
<td>0.51</td>
<td>1.17</td>
<td>2.21</td>
<td>0.23</td>
<td>0.09</td>
<td>0.16</td>
<td>0.05</td>
</tr>
<tr>
<td>SD</td>
<td>1.32</td>
<td>0.50</td>
<td>4.89</td>
<td>1.31</td>
<td>0.23</td>
<td>1.39</td>
<td>2.14</td>
<td>0.42</td>
<td>0.27</td>
<td>0.28</td>
<td>0.18</td>
</tr>
<tr>
<td>1</td>
<td>0.04</td>
<td>0.15</td>
<td>0.04</td>
<td>0.04</td>
<td>0.07</td>
<td>0.02</td>
<td>0.07</td>
<td>0.07</td>
<td>0.03</td>
<td>0.01</td>
<td>0.09</td>
</tr>
<tr>
<td>2</td>
<td>0.12</td>
<td>0.19</td>
<td>0.05</td>
<td>0.07</td>
<td>0.07</td>
<td>0.08</td>
<td>0.09</td>
<td>0.07</td>
<td>0.06</td>
<td>0.01</td>
<td>0.05</td>
</tr>
<tr>
<td>3</td>
<td>0.09</td>
<td>0.10</td>
<td>0.05</td>
<td>0.07</td>
<td>0.03</td>
<td>0.02</td>
<td>0.03</td>
<td>0.03</td>
<td>0.04</td>
<td>0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>4</td>
<td>0.04</td>
<td>0.12</td>
<td>0.09</td>
<td>0.07</td>
<td>0.07</td>
<td>0.06</td>
<td>0.07</td>
<td>0.06</td>
<td>0.05</td>
<td>0.01</td>
<td>0.04</td>
</tr>
<tr>
<td>5</td>
<td>0.05</td>
<td>0.22</td>
<td>0.12</td>
<td>0.05</td>
<td>0.07</td>
<td>0.07</td>
<td>0.06</td>
<td>0.07</td>
<td>0.04</td>
<td>0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>6</td>
<td>0.04</td>
<td>0.01</td>
<td>0.03</td>
<td>0.05</td>
<td>0.05</td>
<td>0.08</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>7</td>
<td>0.02</td>
<td>0.05</td>
<td>0.02</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.01</td>
<td>0.01</td>
<td>0.04</td>
<td>0.02</td>
</tr>
</tbody>
</table>

N=3212; Ind. cap. int.= Industry capital intensity; Ind. concentr.= Industry concentration; Related div.=Related Diversification
We could only explore lags as deep as two because ROA could be calculated for up to 2017 for the observations in 2015.

Additional Analyses

While the above mentioned analysis provides evidence indicating the presence of positive effects of counter-breach initiatives on a firm’s forward-looking and risk-adjusted measures of business value, we further investigate if this positive impact is detectable in a more traditional measure of profitability, i.e., return on assets (ROA). Since a favorable market response to a firm’s security may not impact ROA immediately, we ran a series of models similar to equation (1) with ROA as the dependent variable and all the independent variables included contemporaneously (no lag). Also, we ran models by lagging ANN and ARE variables by one and two years. Table 4 reports the coefficients of ANN and ARE variables in these models. While the impact of counter-breach initiatives on ROA in contemporaneous models and the model with one lag is not statistically significant, the model with two lags presents estimates that follow the same pattern observed in the main analysis, with the exception that the impact of counter-breach initiatives in SS2 remains insignificant and the observed significant effect sizes are slightly smaller than those observed in the main analysis. Overall, these results suggest that while the impacts of counter-breach initiatives are not immediately detectable in more traditional indicators of profitability, the impacts become more visible and tangible over time.

Moreover, the effects of publicly-announced counter-breach initiatives may be heterogeneous depending on the type of initiative a firm engages in. As such, the impact of the publicly-announced counter-breach initiatives may be due to engaging in a certain initiatives but not others. The initiatives included in the dataset fall into the broad categories of: changes in human resources (e.g., changes in recruitment policies or cybersecurity training programs), investment in cybersecurity technologies (e.g., investment in distributed computing), and investment in cybersecurity R&D (e.g., investment in an in-house security lab, investment in cybersecurity startups). Any given announcement may fall into one or more of these categories. To account for the differences across various types of counter-breach initiatives, we coded the category(ies) to which each announcement belongs to and included three dummies of initiative types (i.e., HR, Tech, Cyber_R&D) in our original model 4. The results are reported in Table 4. While the coefficients of HR and Cyber_R&D dummies are positive and significant, the coefficients of ANN and ARE show a similar pattern compared to the original findings, suggesting that above-and-beyond the type of announced initiatives, engaging in counter-breach initiatives creates business value.
Investors may react strongly to his paper compared to our study’s findings. Firms are also positively associated with counting indices of profitability, e.g., ROA, are also positively associated with breaches. Initially, when breaches are relatively rare, initiatives a firm may engage in a series of unannounced countermeasures that are not observed in our sample. Our focus on a market reaction to those initiatives, may involve economic payoffs that are adjusted and forward-looking payoffs of such initiatives can be traced in more traditional indices of profitability when enough time elapses. Finally, our findings suggest that lagged measures of accounting indices of profitability, e.g., ROA, are also positively associated with engaging in counter-breaching initiatives, indicating that the risk-adjusted and forward-looking payoffs of such initiatives can be traced in more traditional indices of profitability when enough time elapses. Further, our findings suggest that lagged measures of accounting indices of profitability, e.g., ROA, are also positively associated with engaging in counter-breaching initiatives, indicating that the risk-adjusted and forward-looking payoffs of such initiatives can be traced in more traditional indices of profitability when enough time elapses. Finally, our additional analyses reveal that human resource and R&D initiatives are met with higher payoffs compared to initiatives that concern investing in counter-breaching technologies, shedding light on the heterogeneities of the value of different types of counter-breaching initiatives that a firm may engage in.

Before discussing the implications of the findings, it is worth acknowledging some limitations of this study. First, our evaluation of the economic impact of counter-breaching initiatives is limited to those that are available publicly. While this methodological choice fits our focus on a market reaction to those initiatives, a firm may engage in a series of unannounced counter-breaching initiatives to protect the integrity of those initiatives. Second, the relationship between the number of security breaches in an industry and investors’ reaction is likely to be nonlinear. Initially, when breaches are relatively rare, investors may react strongly towards breaches. As breaches grow in number, the numbing effect will be amplified. Our linear treatment does not take into account such intricacies. Third, our categorization of counter-breaching announcements does not fully include some of the countermeasures that can be found in the existing literature (Yeh and Chang 2007). While this can be a result of limited announcements we observed in our sample, other types of counter-breaching initiatives that are not observed in our sample may involve economic payoffs that are different in intensity and nature compared to our study’s findings. Lastly, while this study investigated counter-breaching initiatives that are broadcasted publicly through media announcements and annual reports, some counter-breaching initiatives may not be disclosed publicly. Future research may compare the business value of nondisclosed counter-breaching initiatives to examine the generalizability of our findings.

In spite of its limitations, this paper has a few theoretical implications. The study contributes to the literature on economics of information security in three fronts. First, while the prevalence of security

<table>
<thead>
<tr>
<th>Lag Effects</th>
<th>DV= ROA(t)</th>
<th>Low (ss1)</th>
<th>High (ss2)</th>
<th>Low (ss3)</th>
<th>High (ss4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 4.1 (No Lag)</td>
<td>ANN(t)</td>
<td>0.009(0.007)</td>
<td>0.004(0.002)</td>
<td>-0.004(0.002)</td>
<td>0.009(0.005)</td>
</tr>
<tr>
<td></td>
<td>ARE(t)</td>
<td>0.011(0.009)</td>
<td>0.004(0.002)</td>
<td>-0.004(0.002)</td>
<td>0.009(0.006)</td>
</tr>
<tr>
<td>Model 4.2 (1Year Lag)</td>
<td>ANN(t-1)</td>
<td>0.019*(0.010)</td>
<td>0.004(0.003)</td>
<td>0.003(0.002)</td>
<td>0.011(0.007)</td>
</tr>
<tr>
<td></td>
<td>ARE(t-1)</td>
<td>0.018*(0.010)</td>
<td>0.006(0.004)</td>
<td>0.010*(0.006)</td>
<td>0.021*(0.008)</td>
</tr>
<tr>
<td>Model 4.3 (2 Year Lag)</td>
<td>ANN(t-2)</td>
<td>0.031**(0.010)</td>
<td>0.009(0.005)</td>
<td>0.015*(0.006)</td>
<td>0.019*(0.010)</td>
</tr>
<tr>
<td></td>
<td>ARE(t-2)</td>
<td>0.038*(0.017)</td>
<td>0.008(0.005)</td>
<td>0.025*(0.008)</td>
<td>0.041**(0.015)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Controls</th>
<th>DV= Tobin’s q(t)</th>
<th>Low (ss1)</th>
<th>High (ss2)</th>
<th>Low (ss3)</th>
<th>High (ss4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 4.4</td>
<td>ANN(t)</td>
<td>0.096****(0.01)</td>
<td>0.021*(0.009)</td>
<td>0.012*(0.006)</td>
<td>0.061**(0.022)</td>
</tr>
<tr>
<td></td>
<td>ARE(t)</td>
<td>0.058**(0.021)</td>
<td>0.013*(0.007)</td>
<td>0.018*(0.009)</td>
<td>0.034*(0.017)</td>
</tr>
<tr>
<td></td>
<td>HR(t)</td>
<td>0.091****(0.025)</td>
<td>0.024*(0.010)</td>
<td>0.019*(0.011)</td>
<td>0.039**(0.016)</td>
</tr>
<tr>
<td></td>
<td>Tech(t)</td>
<td>0.009(0.006)</td>
<td>0.004(0.003)</td>
<td>-0.003(0.002)</td>
<td>0.008(0.004)</td>
</tr>
<tr>
<td></td>
<td>Cyber_R&amp;D(t)</td>
<td>0.032**(0.010)</td>
<td>0.016*(0.008)</td>
<td>0.012*(0.010)</td>
<td>0.105**(0.019)</td>
</tr>
</tbody>
</table>

|           | N     | 924   | 682     | 1016     | 590       |

*p < 0.10; **p < 0.05; ***p < 0.01; ****p < 0.001. Estimates of industry and year dummies and all other control variables mentioned in equation (1) are used in estimation of these four models, but are excluded for brevity. Standard errors are reported in parentheses. All changes in Wald’s Chi due to the addition of variables are significant at p < 0.001. The coefficients of no lags, 1 year lags, and 2 years lags of ANN and ARE are estimated by running separate regression models.

Table 4. Additional Analyses

Discussion and Conclusion

Overall, the findings of the study suggest that engaging in counter-breaching initiatives is met with economic rewards in the market, although the intensity of such rewards depends on the relative information security level of the focal firm in its institutional environment. Counter-breaching initiatives are most valuable for firms that are under- or over-performing compared to their industry peers. Further, our findings suggest that lagged measures of accounting indices of profitability, e.g., ROA, are also positively associated with engaging in counter-breaching initiatives, indicating that the risk-adjusted and forward-looking payoffs of such initiatives can be traced in more traditional indices of profitability when enough time elapses. Finally, our additional analyses reveal that human resource and R&D initiatives are met with higher payoffs compared to initiatives that concern investing in counter-breaching technologies, shedding light on the heterogeneities of the value of different types of counter-breaching initiatives that a firm may engage in.
breaches casts doubts on the value of reaction mechanisms, we have empirically demonstrated an overall positive effect of counter-breach initiatives on firm profitability. On one hand, the costly nature of security breaches pushes companies to react by engaging in counter-breach measures, and on the other hand, the prevalence of security breaches discourages companies from taking actions. Therefore, recent arguments were made (Kvochko and Pant 2015) that if no firm is safe from security breaches, companies that are less responsive to security breaches could well go unpunished in the stock market. We have unraveled the paradox by showing that counter-breach initiatives indeed have tangible values. Second, this study offers a framework that explains the heterogeneity of the value accrued from engaging in counter-breach initiatives. This study shows that counter-breach initiatives are less valuable if the firm is neither under-performing nor over-performing, in terms of being affected by security threats, relative to its institutional environment. The study’s utilization of BTOF and the legitimacy theory provides a broader view of the differential value of counter-breach initiatives in different environments. Our social comparison account shows that valuation of counter-breach initiatives not only depends on the initiative itself, but also on the relative security level of the firm. While this social comparison account has recently been utilized in studying the value of general IT investments (Ho et al. 2017), we extend its use to understanding the value of investments related to information security.

For managers, this study has revealed a framework to evaluate the promise of counter-breach initiatives. Before engaging in counter-breach initiatives, managers should evaluate the relative security level of their firm vis-à-vis the institutional environment in which they operate. Before committing resources to fight security breaches, organizations need to evaluate their information security strategy. A firm may choose to be a leader in information security in its industry or be merely satisfied by remaining relatively secure. In either case, the market will react by evaluating the firm’s relative stance in the underlying industry. The study also suggests that not all counter-breach initiatives are treated equally in the market. Specifically, while investing in cybersecurity infrastructural technologies may be lucrative, our results suggest that investment in human resources and R&D initiatives related to cybersecurity may lead to higher economic gains. Finally, our study suggests that the profitability benefits of engaging in counter-breach initiatives can be traced in traditional indices of profitability, but managers should allow enough time elapse before they scrutinize their firm’s financial reports to quantify such benefits.

REFERENCES