MIS Quarterly

RESEARCH NOTE

HUMAN CAPITAL ACQUISITION IN RESPONSE TO DATA BREACHES[1]

Sarah H. Bana
George L. Argyros College of Business and Economics, Chapman University, Orange, CA,
and Stanford Digital Economy Lab, Stanford University, Stanford, CA, U.S.A. {sarah.bana@gmail.com}

Erik Brynjolfsson
Stanford Digital Economy Lab, Stanford University, Stanford, CA, and
National Bureau of Economic Research, Cambridge, MA, U.S.A. {erik.brynjolfsson@gmail.com}

Wang Jin
Stanford Digital Economy Lab, Stanford University, Stanford, CA, U.S.A. {jwangjin@stanford.edu}

Sebastian Steffen
Department of Business Analytics, Carroll School of Management, Boston College, Chestnut Hill, MA,
and Stanford Digital Economy Lab, Stanford University, Stanford, CA U.S.A. {sebastian.steffen88@gmail.com}

Xiupeng Wang
D'Amore-McKim School of Business, Northeastern University, Boston, MA,
and Stanford Digital Economy Lab, Stanford University, Stanford, CA, U.S.A. {xiupeng.j.wang@gmail.com}

Given the rise in the frequency and cost of data security threats, it is critical to understand whether and how companies strategically adapt their operational workforce in response to data breaches. We study hiring in the aftermath of data breaches by combining information on data breach events with detailed firm-level job posting data. Using a staggered difference-in-differences approach, we show that breached firms significantly increase their demand for cybersecurity workers. Furthermore, firms' responses to data breaches extend to promptly recruiting public relations personnel—an act aimed at managing trust and alleviating negative publicity—often ahead of cybersecurity hires. Following a breach, the likelihood of firms posting a cybersecurity job rises by approximately two percentage points, which translates to an average willingness to spend an additional $61,961 in annual wages on cybersecurity, public relations, and legal workers. While these hiring adjustments are small for affected firms, they represent a large potential impact of over $300 million on the overall economy. Our findings underscore the vital role of human capital investments in shaping firms' cyber defenses and provide a valuable roadmap for managers and firms navigating cyberthreats in an increasingly digital age.

Keywords: Cybersecurity, data breaches, human capital acquisition, value of data and privacy, incident response, IT strategy

Introduction

The digitization of business activities has led to an ever-increasing amount of digital information. According to World Economic Forum estimates, by 2025, over 460 million terabytes of data will be created each day.[2] The proliferation of digital information has, in turn, led to a rise in data breaches, with over 4,900 breaches in 2022 alone. Billions of exposed individual records, costing $4.45 million per breach on average,[3] have made data protection a top

[1] Corey Angst was the accepting senior editor for this paper. Brad Greenwood served as the associate editor. Authors are listed in alphabetical order and contributed equally.

[2] See https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[3] See https://www.ibm.com/security/digital-assets/cost-data-breach-report.

economic and national security priority for both firms and governments (e.g., Executive Order 13800, 2017; Executive Order 14028, 2021). As hackers and cybercriminals launch more sophisticated attacks, incident response capacities require more sophisticated expertise. Consequently, cybersecurity-related human capital has become an increasingly salient consideration for firms and policymakers alike.

Given rapid digitization and increasingly costly cyberthreats, scholars know surprisingly little about how firms respond internally to data breaches, especially concerning strategic hiring to improve operations after breaches. Discussions about data breaches often concern their implications for external, secondary actors, such as consumers (Athey et al., 2017; Buckman et al., 2018; Janakiraman et al., 2018; Turjeman & Feinberg, 2024), litigators (Romanosky et al., 2014), and the stock market (Acquisti et al., 2006; Richardson et al., 2019). More recently, scholars have documented internal responses that include post-breach technological capital investment (Li et al., 2023), corporate social responsibility contributions (Akey et al., 2023), divestiture of unrelated divisions (Say & Vasudeva, 2020), and turnover at the management level (Banker & Feng, 2019; Say & Vasudeva, 2020). Yet the extent of increased human capital investment at the operational level remains poorly understood, even though it is widely recognized that "employees are [a firm's] first line of defense against cyber attacks" (Toth, 2018). Because complete cyber risk prevention cannot practically be achieved (Gordon et al., 2020; Kaspersky Lab, 2018), it is crucial to gain a deeper understanding of post-breach dynamics.

To address this issue, our paper examines how firms respond internally to data breaches by investing strategically in cybersecurity-related human capital. We bring together breach incident data from Privacy Rights Clearinghouse (PRC) and firm-level data on online job postings from Lightcast to create a novel data set that allows us to analyze post-breach strategic human capital investments. Adopting a difference-in-differences (DiD) design, we found that after a firm suffers a breach, the probability that it will post a cybersecurity role increases by two percentage points, which amounts to an 8% increase for the average breached firms in our sample. This effect persists across a wide range of robustness tests, including matching methods based on industry and pre-data-breach firm characteristics as well as newly developed DiD methods for dynamic treatment effects (Sun & Abraham, 2021).

We also explored hiring responses in public relations (PR) and legal occupations. PR practitioners, who serve as a bridge between the organization, breach victims, and the media, play a pivotal role in mitigating the negative impact of a data breach on a firm's public image (Kim et al., 2017). Legal professionals also play a critical role in incident response, especially when breached firms possess cyber insurance (Talesh, 2018). We found a significant hiring response for PR occupations, a weaker response for legal occupations, and no response for other, non-relevant occupations. In particular, we found that the demand for PR professionals tends to spike significantly in the first quarter following the breach announcement, which may be related to the urgency associated with skilled crisis communication and trust management to reassure stakeholders and mitigate reputational damage.

Our results newly document that firms respond to security lapses by making strategic investments in human capital at the operational level, which is a critical component of strengthening cyber defenses. In addition, we offer practical managerial advice by revealing the common industry hiring practices in response to data breaches, which managers can leverage as a benchmark for their own hiring efforts to ensure they stay ahead of evolving threats. As an empirical extension of our main analyses, we differentiate the types of roles that firms hire in response to data breaches by leveraging the Workforce Framework for Cybersecurity, developed by the National Initiative for Cybersecurity Education (NICE). We found that firms are most likely to increase their hiring in the "Oversee and Govern" category, suggesting a need for cybersecurity leadership and management personnel. This is closely followed by the "Operate and Maintain," "Securely Provision," and "Protect and Defend" categories. In providing these tangible examples of strategic hiring for specific kinds of cybersecurity roles post breach, we help demystify cybersecurity hiring, which may be useful since many firms are inexperienced in hiring cybersecurity-relevant positions.

Overall, our paper highlights the importance of human capital for firms' cyberthreat management. Human capital, as a complement to technological capital, is a fundamental component of firms' internal cyber defenses and day-to-day operations. We show that firms respond to data breaches with strategic and meaningful hiring behavior, by promptly improving their PR capabilities and then by strengthening their internal cybersecurity competencies. Firms' human capital investments in response to data breaches are associated with a willingness to increase average wage bills by $61,961 per year, a relatively small number given that the cost of a breach is over ten times higher (estimated at upwards of $600,000 in costs, including the payment of damages, loss of customers, etc.). By estimating these strategic hiring responses, we provide insight into how firms acquire human capital to prevent data breaches and protect their assets, reputation, and customer trust.

Literature and Hypothesis Development

Most extant studies of data breaches focus on *external* responses to breaches, such as responses by customers (Janakiraman et al., 2018; Kamiya et al., 2021), the stock market (Acquisti et al., 2006; Malhotra & Kubowicz Malhotra, 2011; Martin et al., 2017), and other firms or competitors (Ashraf, 2022). Customers reduce spending in response to data breaches, leading to declines in sales (Janakiraman et al., 2018; Kamiya et al., 2021), but this effect diminishes quickly, even when highly sensitive data has been exposed (Turjeman & Feinberg, 2024). The relatively short-lived nature of these responses aligns with the "privacy paradox" (Athey et al., 2017), which predicts that the importance customers assign to data privacy is contradicted by their actions. This pattern is also evident in investor responses, which are initially negative, resulting in adverse abnormal stock returns for affected firms (e.g., Acquisti et al., 2006; Malhotra & Kubowicz Malhotra, 2011; Martin et al., 2017); but these reactions, too, are typically short-lived and small in scale (Richardson et al., 2019).

Emerging studies on *internal* responses have primarily established that breached firms make changes to their governance and communication strategies. Specifically, firms strategically time breach communication to days when news media are otherwise occupied (Foerderer & Schuetz, 2022). Breached firms also subsequently increase their CTO and CIO turnover (Banker & Feng, 2019; Say & Vasudeva, 2020) and promote board directors with IT expertise (Benaroch & Chernobai, 2017). It is possible that such changes to governance center on image rehabilitation and managerial "scapegoating" (Say & Vasudeva, 2020) that, in theory, could contribute to the short-lived nature of external responses to breaches. Additionally, while managerial adjustments may be an important component of firms' experiences post-breach, they do not necessarily indicate actions that enhance day-to-day cybersecurity at the operational level. Overall, little is known about how firms adjust to cybersecurity incidents at this level.

In the present study, we consider whether and how firms invest in human capital at the operational level after breaches occur. Our emphasis on hiring is significant for at least two reasons. First, although studies show that firms increase spending on IT infrastructure following data breaches (Akey et al., 2023), these physical capital investments may be insufficient to improve cyber-defense operational efficiency if firms lack complementary investments in human capital (Bresnahan et al., 2002). These overlooked operational changes in human capital are necessary because advanced technological solutions require not just physical IT but in-house human expertise for deployment, management, and optimization (Brynjolfsson et al., 2021; Liu et al., 2020). Second, capturing different kinds of hiring contributes to the conversation about firms' priorities following data breaches because it allows us to simultaneously assess the speed and scale of relative human capital investments.

In the current study, we analyze data breach responses by focusing on the underexplored area of firms' hiring for cybersecurity, PR, and legal positions. Cybersecurity professionals are needed not only to assess and contain data breaches but also to implement threat detection systems and security measures that are more advanced and sophisticated than those previously employed. Data breaches often reveal underlying organizational vulnerabilities and thus necessitate both immediate and long-term operational responses (Say & Vasudeva, 2020). Cybersecurity experts are needed to execute and orchestrate these responses. Furthermore, data breaches can shift internal priorities and lead to a greater emphasis on cybersecurity and data governance. In theory, the experience of suffering a breach could encourage firms to address initial vulnerabilities and become more attuned to both the potential risks and consequences of inadequate cybersecurity. All these consequences imply a greater role for cybersecurity talent. Thus, we hypothesize:

H1: *A data breach is associated with an increase in postings for cybersecurity roles at the breached firm*.

The extant literature shows that in the aftermath of data breaches, a firm pays close attention to its communication strategy (Foerderer & Schuetz, 2022). While the reported external responses are mostly modest (Janakiraman et al., 2018; Kamiya et al., 2021), they can, in rare cases, lead to adverse media coverage and loss of trust by customers and business partners (Kelly, 2005). Public relations (PR) experts are thus likely to play an important role in firms, given that they can mitigate the negative impact of data breaches on a firm's public image and mediate public perception (Kim et al., 2017). PR workers can also be involved in interfacing between legal requirements and communication strategies—for example, by identifying an optimal balance between effective communication among different stakeholders and the nondisclosure of sensitive information. Firms may also outsource PR functions to external agencies, but this typically still requires internal PR expertise to ensure that the outsourced activities are in line with the firm's overall communication and legal strategy. In particular, PR workers are needed to fashion apologies to customers that do not admit

guilt, thereby limiting exposure to legal liabilities (Masuch et al., 2021). We expect to find that:

H2: *A data breach is associated with an increase in postings for public relations roles at the breached firm*.

Data breaches not only compromise firms' cybersecurity and public image, they also frequently result in severe legal consequences, such as class-action lawsuits. Legal professionals can play a pivotal role in incident responses, especially when firms impacted by a breach possess cyber insurance (Talesh, 2018). From a legal perspective, breach notification is a major compliance responsibility for firms. Breach notification laws exist in all U.S. states (Vaaler & Greenwood, 2023), but they differ considerably, making compliance highly complex (e.g., they depend on where affected individuals are located). Beyond the legal issues that surround breach notification and direct responses, legal experts can help ensure compliance with other applicable data privacy laws. Thus, we evaluate the following hypothesis:

H3: *A data breach is associated with an increase in postings for legal roles at the breached firm.*

We pose our third hypothesis most tentatively. Although in-house legal professionals have advantages because of their familiarity with firm operations and data systems, firms can, alternatively, consult outside legal experts. That said, we still expect that legal hiring increases will follow breaches, given evidence that cybersecurity is shifting into a domain that relies on the involvement of legal professionals rather than only technical staff (Woods & Ceross, 2021).

Data and Summary Statistics

To test our hypotheses, we combine data on firms' online job postings from Lightcast (formerly Burning Glass Technologies) with information on data breach incidents from Privacy Rights Clearinghouse (PRC).

The Lightcast data covers about 330 million online job vacancy postings posted on over 40,000 distinct online job platforms in the United States between 2010 and 2020. Indeed, it arguably covers the "near-universe" of job postings. Each vacancy posting is parsed, deduplicated, and annotated with the posting date, an occupational SOC code, an industry NAICS code, the employer, and the skills demanded, as well as several other variables. These job postings are scraped daily, which allowed us to capture hiring changes on a high-frequency basis. Researchers have used this data as a measure of labor demand (e.g., Bai et al., 2020; Bana et al., 2023; Deming & Kahn, 2018). We aggregated these demands to the firm-month level and created a balanced panel of firm-month-level demands for workers in cybersecurity, PR, and legal occupations.[4]

PRC sources its data primarily from state attorneys general and the U.S. Department of Health and Human Services offices. It contains over 9,000 data breach events, exposing over 10 billion individual records between 2005 and 2019. This data includes breaches that were reported in compliance with states' data breach notification laws. PRC data provides announcement dates, names of affected organizations, and types of breach events and covers organizations in a wide range of industries.

To ensure the quality of the job posting data, our study's sample includes all firms that had at least 100 job postings in the Lightcast data from 2010 to 2020, though our results are robust to different cutoffs. Among a total of over 89,000 organizations, through a series of matching procedures, we identified 1,493 firms that experienced data breaches.[5]

Panel A in Table 1 presents summary statistics for the firms in our "non-breached," "breached," and "overall" samples. Non-breached and breached firms served as our control group and treatment group, respectively, for the DiD setting. To mitigate potential confounding factors such as firm experience with data breaches, we selected the first data breach event that a firm experienced during our sample period as the treatment. Our final sample included 1,493 firms that experienced any form of data breach (i.e., "breached"). Among them, 1,346 (90%) posted at least one job for cybersecurity occupations, 1,074 (72%) posted at least one job for PR occupations, and 1,002 (67%) posted at least one job for legal occupations. 87,628 firms in our sample did not suffer a data breach, and 61,797 (70.5%) of them posted cybersecurity jobs (i.e., "non-breached"). Every month, firms in the control group posted, on average, 12.2 jobs; of these, 0.3 postings demanded cybersecurity expertise. In contrast, firms in the treated group posted 144 jobs each month; 3.5 of them asked for cybersecurity expertise. This large difference in postings highlights that breached firms are primarily large firms, which suggests a potential need for propensity score matching.

[4] We report the list of specific SOC codes for each category in Appendix Table A1.

[5] Details of our matching procedures can be found in the Appendix.

Table 1. Summary Statistics			
Panel A: Full sample			
Variables	**Non-breached**	**Breached**	**Overall**
Average number of job postings	12.24	144.0	14.44
Average number of cybersecurity job postings	0.320	3.542	0.374
Average number of PR job postings	0.029	0.324	0.034
Average number of legal job postings	0.047	0.522	0.055
Average number of non-relevant job postings	11.84	139.6	13.98
Average probability of cybersecurity job postings	0.079	0.258	0.082
Average probability of PR job postings	0.016	0.104	0.018
Average probability of legal job postings	0.018	0.096	0.020
Average probability of non-relevant job postings	0.441	0.694	0.446
Number of firms	87,628	1,493	89,121
Firms with cybersecurity postings	61,797	1,346	63,143
Firms with PR postings	36,044	1,074	37,118
Firms with legal postings	29,061	1,002	30,063
Panel B: Breached firms			
Variables	**Pre-breach**	**Post-breach**	**Change**
Average number of job postings	108.7	125.0	+15.0%**
Average number of cybersecurity job postings	2.305	2.892	+25.5%**
Average Number of PR job postings	0.186	0.227	+21.7%**
Average number of legal job postings	0.249	0.326	+30.6%**
Average number of non-relevant job postings	105.9	121.5	+14.7%**
Average probability of cybersecurity job postings	0.234	0.269	+14.8%***
Average probability of PR job postings	0.082	0.097	+18.3%***
Average probability of legal job postings	0.079	0.092	+16.7%***
Average probability of non-relevant job postings	0.670	0.715	+6.7%***

Note: Observations are at the firm-month level. Panel A describes the full sample for both non-breached (control) and breached (treated) firms. Cybersecurity, PR, and legal jobs are defined by the occupations listed in Appendix Table A1. Panel B presents results for breached firms, comparing their hiring behavior four quarters before and four quarters after suffering a data breach. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Empirical Methods

By adopting a DiD design, we explore how, among breached firms (i.e., "treated firms"), changes in the number of jobs posted before and after breach events differ from firms that did not experience a breach (i.e., "control firms"). Because firms cannot perfectly predict the timing of data breaches, breached firms should act similarly to non-breached firms prior to the breach. This allowed us to identify firms' strategic human capital acquisitions in response to data breaches.[6] Formally, our baseline DiD model is specified as follows:

$$Job_{i,j,t} = \beta_0 + \beta_1 D_{i,t} + X_{i,j,t} + \varepsilon_{i,j,t}, \quad (1)$$

where for each firm i in two-digit NAICS industry j and time period t, $Job_{i,j,t}$ is a variable indicating whether the firm posts job vacancies for a specific occupation of interest. $D_{i,t}$ represents a binary variable—"After × Breached"—which equals 1 after a breach occurs and 0 otherwise. Observations in our data are at the firm-month level. $X_{i,j,t}$ is a vector of fixed effects that include firm fixed effects (to control for time-invariant firm heterogeneity), month fixed effects (to control for changes in average posting behavior over time), and calendar month by two-digit NAICS industry fixed effects (to capture time-varying industry-specific unobservable variables, such as seasonality). Standard errors are clustered at the firm level to accommodate intrafirm correlation across time periods (Bertrand et al., 2004; Abadie et al., 2023). We focused on the four quarters before and the four quarters after each data breach event.

One underlying assumption needed for the classical DiD estimation to be valid is that in the absence of a breach, treated firms will exhibit a posting pattern similar to that of the non-breached firms. This assumption cannot be tested because the counterfactual is unobservable. However, we can examine the

[6] While firms can, of course, preemptively improve their defenses, it is widely believed that perfect security is impossible and that every firm faces a non-zero risk of being breached (Gordon et al., 2020; Kaspersky Lab, 2018).

posting behavior of treated and untreated firms before the breach to perform a parallel trends test.

We conducted our parallel trends test at the quarterly level, analogous to our baseline specification, except that we replaced the $D_{i,t}$ (Pre/Post) indicator with a vector of quarterly indicators $D_{i,t+p}$, where $p \in [-3, 4]$ indicates quarters relative to the data breach event. Quarter 0 covers the month of the announcement of the data breach event, along with the two preceding months, and Quarter -1 is used as the omitted category (Freyaldenhoven et al., 2021).

We selected quarterly analysis in the parallel trends test for two reasons. First, firms receive no strategic benefit from delaying their hiring investment responses, but they can benefit from delaying the public announcement. In the United States, data breach notification laws allow for reasonable reporting delays, typically up to three months (see Foerderer & Schuetz, 2022 and Appendix Figure A1). Thus, firms can hire in response to data breaches up to three months *prior* to publicly reporting those breaches. Second, as demonstrated in Table 1, firms in our sample posted, on average, fewer than one cybersecurity, PR, and legal job posting within a given month, with considerable monthly variation. Therefore, our preferred specification contains quarterly indicators to smooth out short-term fluctuations, although we also report results at the monthly level to examine dynamic response timing in Appendix Figures A2-A4.

We also conducted a series of robustness checks. First, although our identification strategy exploits the unanticipated timing of the data breach events, post-event labor demand could potentially be driven by other pre-breach, firm-level time-varying characteristics, such as prior hiring behavior, which could lead to biased estimates. Thus, we performed propensity score matching (PSM) to construct a sample that consisted of similar firms identified based on pre-breach firm-level observables. That is, we matched firms based on their industry, as well as their accumulative total labor demand (a proxy for firm size), cumulative demand for cybersecurity, PR, and legal workers during the year prior to a particular cohort (e.g., the year when the data breach event happened). We matched the treatment and control groups through the nearest neighbor method and imposed common support with five neighbors and a 0.001 caliper.

Second, staggered treatment timing (i.e., the varied timing of data breach events) could lead to contamination issues in our baseline DiD estimates. Recent literature has shown that in settings with variation in treatment timing across units with heterogeneous treatment effects, coefficients on a given lead or lag can be contaminated by effects from other time periods (Callaway & Sant'Anna, 2021; Sun & Abraham, 2021). Although the significantly larger size of our control group can help to minimize such biases (Goodman-Bacon, 2021), to tackle this issue we applied the newly developed Sun and Abraham estimator, hereafter referred to as the S&A estimator.[7] Third, we used a Poisson model to explicitly model the number of job postings as a non-negative count outcome variable. Finally, to mitigate issues that can stem from imprecise treatment timing, we performed additional regressions that exclude quarter zero but include an additional preceding quarter (e.g., Quarter -2). The description and summary of findings for all robustness tests are presented in Table 8.

Results

Effect of Data Breaches on Hiring for Cybersecurity

We first examined whether, following a data breach, firms strengthen their cybersecurity workforce. Table 2 reports results using both (1) indicators for having posted a cybersecurity role (Columns 1 to 3) and (2) counts (Columns 4 and 5) as outcome variables.

Column 1 presents the result for a two-period DiD model in which the dependent variable is an indicator of whether the firm posts cybersecurity jobs. The variable of interest, "After × Breached," is an indicator that equals 1 for breached firms after the announcement of the data breach event. Its coefficient in Column 1 indicates that, compared to non-breached firms during the same time window, firms increase their probability of posting cybersecurity jobs by 2.2 percentage points after a breach. This effect is statistically significant at the 1% level. Combining this increase with the pre-breach mean for treated firms, our finding implies that firms have a 9.4% (0.022/0.234) increased probability of posting a cybersecurity job after experiencing a data breach.

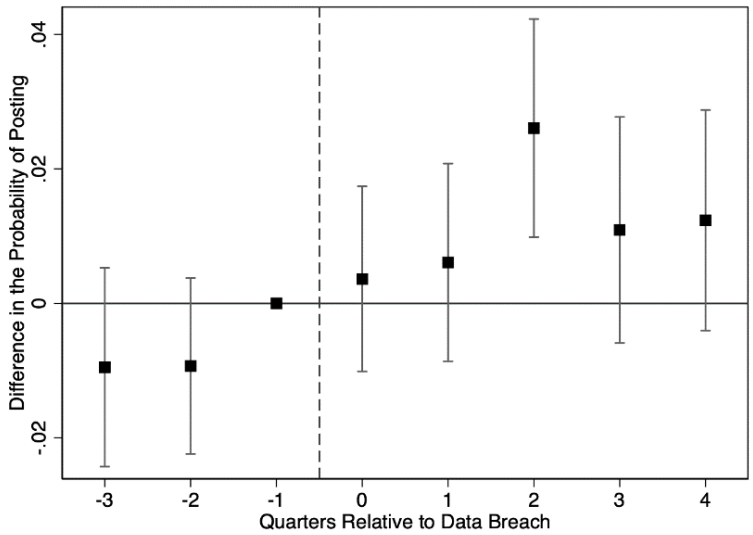
In the next column, we present similar results based on a matched sample. The most restrictive specification used the S&A staggered DiD estimator with the matched sample and is presented in Column 3. The estimated coefficient of 1.7 percentage points implies a 7.9% (0.017/0.216) effect for the treated and resembles those presented in Columns 1 and 2, further validating our baseline findings.

[7] Essentially, the new estimator estimates the shares of cohorts as weights and, thus, allows the resulting weighted average of treatment effects to extend beyond a convex combination of treatment effects. For additional details, please see Goodman-Bacon (2021), Słoczyński (2022), and Sun and Abraham (2021).

Table 2. Effect of Data Breaches on Hiring for Cybersecurity Talent

Models	Probability			Counts	
Variables	(1) Full sample	(2) Matched sample	(3) Matched sample Sun & Abraham	(4) Full sample	(5) Full sample Poisson
After × Breached	0.022*** (0.005)	0.020*** (0.007)	0.017** (0.006)	0.512*** (0.144)	1.087* (0.048)
R-squared	0.308	0.419	0.415	0.432	-
# of firms	89,121	5,077	5,077	89,121	59,503
$\bar{Y}$ pre-breach	0.234	0.216	0.216	2.305	3.590

Note: Columns 1 to 4 include firm, month, and calendar-month-by-sector fixed effects. Column 5 includes firm, year, month, and sector fixed effects. The dependent variables for Columns 1 to 3 are indicators of whether the firm posts cybersecurity jobs; the dependent variable for Columns 4 to 5 is the number of cybersecurity jobs that a firm posts. The coefficient for Column 5 is reported as an incidence rate ratio (IRR). Standard errors are clustered at the firm level. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.



Note: Figure 1 displays the parallel trends test described in the Empirical Methods section, using the quarterly dynamics coefficients and applying the S&A estimator to the matched sample. Quarter 0 includes months -2, -1, and 0. Quarter -1 is the omitted category. The reported 95 percent confidence intervals use standard errors clustered at the firm level.

Figure 1. Quarterly Dynamics for Cybersecurity Hiring (± 4 Quarters Around Breach)

Thus far, we have primarily focused on the relationship between data breaches and the likelihood of increased cybersecurity-related hiring. We were also interested in the effect of data breaches on the actual *number* of cybersecurity job postings; the results are reported in Columns 4 and 5 of Table 2. We found that breached firms, on average, exhibited an increase of 0.5 cybersecurity-related job postings after a breach event. The Poisson regression in Column 5 further confirms these post-breach increases. The reported incidence rate ratio (IRR) of 1.087 implies that following a breach, and compared to non-breached firms, breached firms exhibited an 8.7% increase, on average, in the number of cybersecurity postings. Overall, the results in Table 2 strongly support our first hypothesis (H1).

To test the parallel trend assumption and better understand the timing of strategic hiring decisions made in response to data breaches, we moved beyond our pre-post baseline comparison and analyzed the dynamics in firms' cybersecurity posting behavior using the preferred S&A estimator on our matched sample. The results are visualized in Figure 1.[8]

[8] For robustness, we also analyzed quarterly parallel trends by applying the conventional DiD estimator to the matched sample (see Appendix Table A5). Those results are largely consistent with the ones reported here.

The base period (omitted category) for comparison is Quarter -1. The results confirm pre-breach parallel trends: the probability of posting a cybersecurity job for breached firms is not statistically different from non-breached firms before a data breach event. However, breached firms are significantly more likely to post cybersecurity jobs after breach events. The effect size increases to 2.6 percentage points in Quarter +2. These results are consistent with our baseline results from Columns 1 to 3 in Table 2.

Effect of Data Breaches on Hiring for Public Relations

As discussed in H2, in response to data breaches, firms might increase their demand for PR professionals who can manage their brand image, handle external communication, counter negative media attention, and improve public trust. Using the same methodology as in Table 2, we tested H2 and present the results in Table 3.

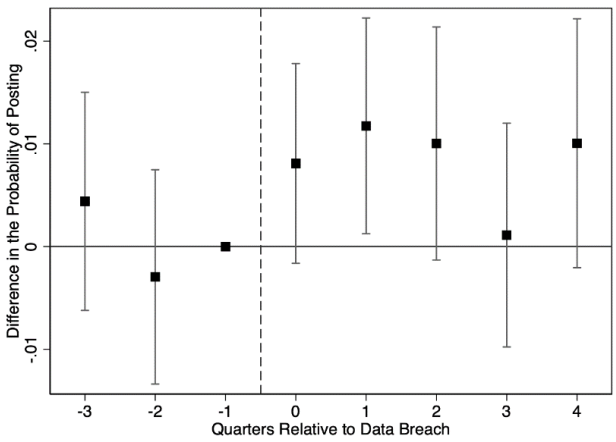
Similar to Table 2, Columns 1 to 3 in Table 3 present results from a two-period DiD model for indicators of having posted a PR role. The results in these columns consistently show that following a data breach, breached firms are about 1 percentage point more likely than non-breached firms to demand PR roles, though this effect is slightly weaker in Columns 2 and 3 possibly due to a much smaller sample. However, the models from Columns 4 and 5 reveal a null effect on the actual counts of PR postings, suggesting that data breaches primarily prompt firms to decide *whether* to hire for PR rather than *how many* PR specialists to hire.

Following our analysis of cybersecurity hiring, we explore the dynamics of the effect and visualize the results in Figure 2. This figure, which applies the S&A estimator to the matched sample, shows that firms significantly increase their probability of hiring for PR during Quarter +1, shortly after the breach announcement.

Table 3. Effect of Data Breaches on Hiring for Public Relations Talent

Models	Probability			Counts	
Variables	(1) Full sample	(2) Matched sample	(3) Matched sample Sun & Abraham	(4) Full sample	(5) Full sample Poisson
After × Breached	0.010***	0.008*	0.008*	0.024	0.991
	(0.003)	(0.004)	(0.004)	(0.028)	(0.118)
R-squared	0.172	0.280	0.274	0.237	-
# of firms	89,121	5,077	5,077	89,121	32,526
$\bar{Y}$ pre-breach	0.082	0.080	0.080	0.186	0.473

Note: Columns 1 to 4 include firm, month, and calendar-month-by-sector fixed effects. Column 5 includes firm, year, month, and sector fixed effects. The dependent variables for Columns 1 to 3 are indicators of whether the firm posts public relations jobs; the dependent variable for Columns 4 to 5 is the number of public relations jobs that a firm posts. The coefficient for Column 5 is reported as an incidence rate ratio (IRR). Standard errors are clustered at the firm level. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.



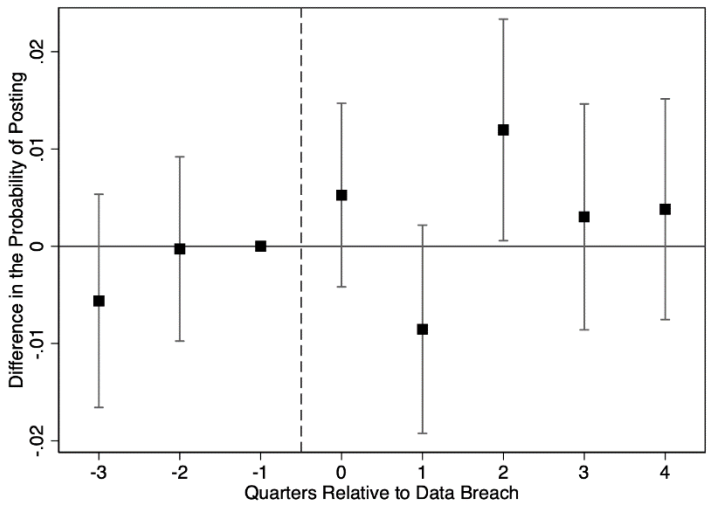
Note: Figure 2 displays the parallel trends test described in the Empirical Methods section, using the quarterly dynamics coefficients and the S&A estimator with the matched sample. Quarter 0 includes months relative to the breach -2, -1, and 0. Quarter -1 is the omitted category. The reported 95% confidence intervals use standard errors clustered at the firm level.

Figure 2. Quarterly Dynamics for PR Hiring (± 4 Quarters Around Breach)

Table 4. Effect of Data Breaches on Hiring for Legal Talent

Models	Probability			Counts	
Variables	(1) Full sample	(2) Matched sample	(3) Matched sample Sun & Abraham	(4) Full sample	(5) Full sample Poisson
After × Breached	0.008**	0.004	0.006	0.058***	1.033
	(0.003)	(0.004)	(0.004)	(0.019)	(0.122)
R-squared	0.246	0.334	0.329	0.236	-
# of firms	89,121	5,077	5,077	89,121	26,223
$\bar{Y}$ pre-breach	0.079	0.077	0.077	0.249	0.698

Note: Columns 1 to 4 include firm, month, and calendar-month-by-sector fixed effects. Column 5 includes firm, year, month, and sector fixed effects. The dependent variables for Columns 1 to 3 are indicators of whether the firm posts legal jobs; the dependent variable for Columns 4 to 5 is the number of legal jobs that a firm posts. The coefficient for Column 5 is reported as an incidence rate ratio (IRR). Standard errors are clustered at the firm level. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.



Note: Figure 3 displays the parallel trends test described in the Empirical Methods section, using the quarterly dynamics coefficients and the S&A estimator with the matched sample. Quarter 0 includes months relative to the breach -2, -1, and 0. Quarter -1 is the omitted category. The reported 95% confidence intervals use standard errors clustered at the firm level.

Figure 3. Quarterly Dynamics for Legal Hiring (± 4 Quarters Around Breach)

This finding confirms H2, that to deal with public scrutiny following a data breach, firms increase their demand for PR. More interestingly, the PR response is relatively quick: the hiring effect for PR shows up one quarter after the breach, while the effect for cybersecurity is strongest two quarters after the breach.

Effect of Data Breaches on Hiring for Legal

Next, we investigated H3 by exploring the effect of data breaches on firms' demand for legal roles using the same methods as in Tables 2 and 3. The results are presented in Table 4. We found that the results were weaker for the hiring of legal professionals. As the first three columns reveal, there was no significant difference between breached and non-breached firms in the probability of hiring legal workers using the matched sample. When using the number of legal job postings as the outcome variable (Columns 4-5) our results were mixed and noisy.

To again investigate the dynamics of the effect on legal hiring we applied the S&A estimator to the matched sample. The results, presented in Figure 3, largely confirm the results in Columns 1-3 of Table 4, showing a mild increase in Quarter +2. Overall, the results from our analysis for legal hiring do not consistently reject the null hypothesis in H3. The disparity in results may be an outcome of the variety of approaches that firms employ after a data breach. Cyber insurance, which can incentivize firms to outsource legal work (Woods et al., 2023), may be a relevant factor that cannot be controlled for in the currently available data.

Table 5. Effect Heterogeneity Between Cyber and Non-Cyber Events

Models	Cybersecurity		PR		Legal	
Variables	(1) Cyber	(2) Non-cyber	(3) Cyber	(4) Non-cyber	(5) Cyber	(6) Non-cyber
After × Breached	0.040*** (0.009)	0.014 (0.009)	0.009* (0.006)	0.016*** (0.005)	0.006 (0.006)	0.012** (0.006)
p-value on Δ	0.036**		0.409		0.478	
R-squared	0.306	0.306	0.170	0.169	0.243	0.243
# of firms	88,078	88,058	88,078	88,058	88,078	88,058

Note: All regressions include firm, month, and calendar-month-by-sector fixed effects. Columns 1, 3, and 5 only include data breaches that are categorized as cyber attacks; Columns 2, 4, and 6 only include data breaches that are categorized as non-cyber attacks. Standard errors are clustered at the firm level. The *p*-values on the differences are calculated by testing the equality of the coefficients across both regressions. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Tests of Heterogeneous Effects

Differences in Breach Event Type (Cyber vs. Non-Cyber)

To further investigate how firms react to different types of data breach events (particularly those due to cyber vulnerabilities), we split the breaches into cyber attacks and non-cyber attacks. Cyber attacks include a loss of digital data due to hacks by an outside party, malware infections, or digital fraud involving debit or credit cards. The results are presented in Table 5. As shown in Column 1, compared to non-breached firms, breached firms experience a four percentage point increase in their probability of hiring cybersecurity roles. In contrast, the results in Column 2 show that after experiencing a non-cyber attack, firms do not take such cybersecurity hiring actions, and this difference in hiring between breach types is statistically significant. This further supports our first hypothesis and confirms that firms hire strategically and recognize that cyber talent is most needed when defending against cyber-related vulnerabilities.

Interestingly, firms' hiring for PR appears to be much weaker (Columns 3 and 4) after both types of breaches. While statistically significant overall, firms' PR hiring responses did not differ across breach types. While firms' legal hiring responses were not significant overall, Columns 5 and 6 show that non-cyber events may induce stronger responses than cyber events, though these response strength differences could not be statistically distinguished. Overall, these findings offer reassurance that our previously estimated cybersecurity hiring responses are predominantly due to cyber breaches. They further highlight that firms hire strategically and target specific roles based on their internal needs.

Differences in Occupational Hiring Experience

Next, we examined whether the identified hiring responses vary based on firms' prior hiring experience with relevant occupations. Organizations with a history of hiring cyber professionals are better equipped to proactively address and mitigate the impact of data breaches, having established a foundation of cybersecurity knowledge within their workforce. Firms that lack experience in hiring cyber-related workers may be more susceptible to responding inadequately to data breaches due to a lack of dedicated expertise. Conversely, due to their lack of relevant workers, they may also have a greater need to build up their internal cybersecurity operations.

In our empirical analysis, we categorized firms' hiring experience based on their cyber-related posting history. We labeled a firm as "experienced" if it ever posted for positions in the corresponding occupations prior to a breach, and "inexperienced" otherwise, based on hiring histories beginning in 2010. The results are presented in Table 6. Columns 1 and 2 show, respectively, the results for cybersecurity hiring for firms with and without a history of hiring for cybersecurity roles. Inexperienced firms have stronger post-breach responses. Moreover, while inexperienced firms tend to hire for all relevant occupations in response to data breaches, experienced firms focus on cybersecurity workers. However, these differences by firms' experience levels are not statistically significant.

Empirical Extensions

Empirical Extension: Wage Bill Estimation

Thus far, our analysis has focused on quantifying the impact of data breaches through the response they induce on the probability and number of jobs posted by affected firms. To better understand the economic magnitude of these hiring responses, we estimated their implied wage bill increases associated with potential new hires in monetary terms. Since reliable wage information is often absent from job postings (Batra et al., 2023), we conducted this analysis by combining average annual wages at the occupation level from the Bureau of Labor Statistics' Occupational Employment and Wage Statistics (OEWS) with the number of job postings for related occupations.

Table 6. Effect Heterogeneity Between Inexperienced and Experienced Firms

Models	Cybersecurity		PR		Legal	
Variables	(1) Inexperienced	(2) Experienced	(3) Inexperienced	(4) Experienced	(5) Inexperienced	(6) Experienced
After × Breached	0.030*** (0.004)	0.018** (0.007)	0.012*** (0.002)	0.006 (0.007)	0.012*** (0.002)	0.001 (0.008)
p-value on Δ	0.361		0.350		0.221	
R-squared	0.305	0.308	0.168	0.172	0.242	0.246
# of firms	88,120	88,524	88,458	88,186	88,501	88,143

Note: All regressions include firm, month, and month-sector fixed effects. Columns 1, 3, and 5 only include firms that are categorized as inexperienced; Columns 2, 4, and 6 only include firms that are categorized as experienced. Standard errors are clustered at the firm level. The *p*-values on the differences are calculated by testing the equality of the coefficients across both regressions. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Table 7. Most Representative Job Titles

NICE category	Most representative job titles
Oversee & Govern	Director of information technology (6%), security manager (5.2%), information technology auditor (4.1%)
Protect & Defend	Security analyst (12.4%), security engineer (7.9%), information security analyst (6.6%)
Investigate	Security specialist (8.6%), security analyst (8.6%), security engineer (6.7%)
Analyze	Security engineer (10%), security analyst (9.4%), information security analyst (5%)
Operate & Maintain	Network engineer (5.1%), security engineer (5%), systems engineer (4.5%)
Collect & Operate	Systems engineer (5.6%), network engineer (5.2%), security analyst (5%)
Securely Provision	Security engineer (7%), software development engineer (5.5%), network engineer (5.1%)

We estimated Equation (1), our main regression specification, with the wage bills associated with cybersecurity, PR, and legal hiring. We found that a data breach is associated with a $61,961 increase in the total wage bill due to these three occupational categories. Most of this willingness to increase wage bills is attributable to cybersecurity roles (a $52,010 increase), with smaller effects for PR and legal hiring. Considering estimates of average breach costs ranging from $682,650 (Ponemon Institute, 2020) up to $4.5 million,[3] this amount is consistent with a small but discernable increase in cybersecurity investment following a breach. On the other hand, with PRC reporting 4,918 breaches in 2022, this could suggest a potential annual impact of over $300 million on the overall economy.

Empirical Extension: Effect of Data Breaches on Hiring for NICE Functions

To offer detailed insights for companies looking to bolster their cybersecurity capabilities in the aftermath of data breaches, we integrated job posting data with categories in the NICE framework and identified the specific roles that breached firms seek to fill within the NICE cybersecurity functions.[9] To provide actionable managerial insights, we highlight the most representative job titles in Table 7. Each row corresponds to one of the seven categories in the NICE cybersecurity framework.[10]

Summary of Additional Robustness Checks

To further test the robustness of our results, we conducted a series of supplementary analyses. In Table 8, we provide a detailed summary of the potential concerns these robustness checks address and present the corresponding findings.

Discussion

Firms are increasingly relying on data as a critical resource to extract economic value, but they also face growing threats to their ability to safeguard data as cybercrimes become more common and sophisticated. As cybercrimes continue to disrupt businesses, infringe upon privacy, and threaten both public safety and national security, the U.S. has entered a decisive time for shoring up cyber defenses. A recent briefing from the White House identified cyber defense as a national priority and called for more intentional strategies to promote cybersecurity, such as by strengthening the cyber workforce (Executive Order 14028, 2021).

[9] Appendix Figure A1 shows the correlation between our occupation-based definitions of cybersecurity, PR, and legal and the task-based definitions of the seven NICE categories.

[10] For additional regression results based on the NICE framework, as an alternative definition of cybersecurity, see Appendix Table A7.

Table 8. Summary of Additional Robustness Checks

Concerns	Tests and results of additional analyses	Location	Passed?
Firms may strategically delay the announcement of data breaches.	Test: Alternative benchmark period (excluding Quarter 0). Findings: Results are similar to those reported in Tables 2-4.	Table A2	✓
Time window may be inappropriate.	Test: Alternative time window of two quarters before and after data breaches. Findings: Results are similar to those reported in Tables 2-4.	Table A3	✓
Linear probability model may produce predicted probabilities outside the supported range [0,1].	Test: Logit models (both pre/post and quarterly dynamics). Findings: Results are statistically significant and similar to those in Tables 2-4.	Table A4	✓
Counterfactual "control" firms may not be an appropriate comparison group.	Test: Quarterly dynamic models with propensity score matched sample. Findings: Results are consistent with those reported in Figures 1-3.	Table A5	✓
Identified demand increases may coincide with other firm-level shocks and may not be limited to data breach-relevant hiring.	Test: Estimate baseline model using non-relevant jobs (occupations excluding cybersecurity, legal, and PR) as the dependent variable (placebo test). Findings: No significant demand increases in non-relevant occupations.	Table A6	✓
Occupational definitions of cybersecurity-related workers may be inappropriate.	Test: Alternative definition of cybersecurity based on the NICE framework. Findings: Positive correlation between definitions. Comparable results, as in Table 2.	Figure A5, Table A7	✓
Quarterly results may hide monthly heterogeneity.	Test: Monthly dynamic models with propensity score matched sample. Findings: No pre-trends; Results are consistent with those in Tables 2-4.	Figures A2-A4	✓

However, scholars and policymakers know very little about how firms make changes to their operational workforce following data breaches, in part due to a lack of data. In this study, we created a novel dataset on firms' human capital investment strategies by combining firm-level job posting data with information on data breach events. We found that breached firms increase their demand for cybersecurity and PR workers and that the latter response occurs more promptly.

In contrast to existing studies on firms' internal responses to breaches, which focus on IT investments and executive hiring and turnover, we document changes to firms' hiring plans for the operative employees who are ultimately responsible for firms' daily cyber protection. Specifically, we found that hiring for cybersecurity workers increases by two percentage points in the aftermath of a breach—an eight percent increase—and that this occurs primarily in the second quarter after the breach. We also found that hiring for PR workers increases by 0.8 percentage points—a 10% increase—and that this effect tends to occur in the first quarter after the breach. The observed impact on the hiring of legal workers is less consistent. The timing of these effects suggests that firms identify an immediate need to respond to breaches by boosting PR rather than a more delayed need to grow their cybersecurity workforce with a longer horizon in mind. These increased hiring intentions correspond to additional annual labor costs of about $61,961 for each breached firm, which translates to over $300 million for 2022, which saw 4,918 breaches.

We also looked at the extent to which increases in hiring for cybersecurity, PR, and legal workers depend on firms' existing workforces. Among firms that have not hired such workers in the past, the response is generally more

pronounced. This interpretation of our findings suggests that data breaches serve as a source of organizational learning for firms and that human capital investments are an important part of this learning.

From a policy perspective, this kind of learning can present an opportunity. A large share of U.S. firms still lacks cybersecurity expertise: for a sizeable share (about 30%) of firms in our data, we did not observe any hiring of cybersecurity personnel over a 10-year period. If breaches trigger investments that ought to be made for the public good but are otherwise not made, then policymakers could lean into the firm learning that occurs during these events. Furthermore, lessons learned from breached firms can help managers enhance cybersecurity preparedness by anticipating cybersecurity needs. By making the types and scale of hiring that occur post-breach more concrete, our work can empower firms to anticipate and respond more quickly to unexpected cybersecurity threats. In the best case, our work could motivate preemptive hiring before breaches among firms that are otherwise inexperienced when it comes to cybersecurity and may need a place to start.

To that end, our results illustrate to managers what breached firms perceive to be the strategic scale of investment and may provide an initial benchmark to which firms can compare themselves. While we primarily focus on key occupational groups in our main analyses—cybersecurity, PR, and legal hiring—our supplemental analyses using the NICE framework show that firms focus particularly on post-breach improvements in the "Oversee and Govern," "Protect and Defend," "Securely Provision," and "Operate and Maintain" categories (and specific roles such as director of information technology, security analyst, and security engineer).

While our study offers important insights into firms' internal human capital responses, the data we analyze is inherently limited. The Lightcast job posting data did not allow us to directly observe firms' workforce, nor subsequent hires, layoffs, turnover, or multiple jobs being offered through the same job posting. To address these issues, future research will require data on firms' workforces and their workers' roles. Job postings may also be merely symbolic, though this is less likely for hiring at the operational level compared to the executive level. Data on job postings may also overlook the possible impact of outsourced labor. A better understanding of such indirect human (and other) capital investments promises to be a fruitful direction for future research. In addition, breach data from PRC relies on compliance with data breach notification laws and may miss unreported breaches or breaches of intellectual property. In light of the recent progress of generative AI, it is likely that phishing, scamming, and social engineering attacks will become more sophisticated. Another promising direction therefore lies in further differentiating between the value of human capital acquisition and the value of improvements to existing, internal human and technological capital, such as through cybersecurity training programs or AI-aided worker security tools.

In conclusion, our study investigates the strategic human capital investments that firms make in response to data breaches. Given that cybersecurity and data protection are important ongoing concerns, we emphasize that additional research is needed to better understand the phenomenon of data breaches and the human, technological, and other capital investments that firms make to combat them.

Acknowledgments

We thank Bledi Taska, Will Markow, Caroline Effinger, and the Lightcast team for access to and insights on the job posting data. We further thank Linda Zhao, Sam Ransbotham, Daniel Woods, three anonymous WEIS conference reviewers, and our WISE discussant Brad Greenwood for their valuable comments. We also benefited from early feedback from the Cybersecurity at MIT Sloan (CAMS) research group, especially from Keman Huang, Stuart Madnick, Michael Siegel, and Keri Pearlson. We thank the participants of the Conference on Information Systems and Technology (CIST) 2020, the Workshop on Information Systems and Economics (WISE) 2021, the Workshop on the Economics of Information Security (WEIS) 2022, and the American Economic Association (AEA) Annual Meeting 2022 for their thoughtful questions and comments. Funding for this study was provided by a Boston College Kelly Grant and the Stanford Digital Economy Lab.

References

Abadie, A., Athey, S., Imbens, G. W., & Wooldridge, J. M. (2023). When should you adjust standard errors for clustering? *The Quarterly Journal of Economics*, *138*(1), 1-35. https://doi.org/10.1093/qje/qjac038

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the International Conference on Information Systems*. https://aisel.aisnet.org/icis2006/94

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2023). *Hacking corporate reputations* (Rotman School of Management working paper). SSRN. http://dx.doi.org/10.2139/ssrn.3143740

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, *97*(2), 1-24. https://doi.org/10.2308/TAR-2019-1033

Athey, S., Catalini, C., & Tucker, C. (2017). *The digital privacy paradox: small money, small costs, small talk.* National Bureau of Economic Research. https://doi.org/10.3386/w23488

Bai, J., Jin, W., Steffen, S., & Wan, C. (2020). *The future of work: Work from home preparedness and firm resilience during the COVID-19 pandemic.* SSRN. https://dx.doi.org/10.2139/ssrn.3616893

Bana, S., Brynjolfsson, E., Rock, D., & Steffen, S. (2023). work2vec: Measuring the Latent Structure of the Labor Market. In

Proceedings of the American Economic Association Annual Meeting. https://www.aeaweb.org/conference/2023/program/1310

Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems*, *33*(3), 309-329. https://doi.org/10.2308/isys-52532

Batra, H., Michaud, A., & Mongey, S. (2023). *Online job posts contain very little wage information.* National Bureau of Economic Research. https://doi.org/10.3386/w31984

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quarterly*, *41*(3), 729-762. https://doi.org/10.25300/MISQ/2017/41.3.04

Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How Much Should We Trust Differences-In-Differences Estimates? *The Quarterly Journal of Economics*, *119*(1), 249-275. https://doi.org/10.1162/003355304772839588

Bresnahan, T. F., Brynjolfsson, E., & Hitt, L. M. (2002). Information Technology, Workplace Organization, and the Demand for Skilled Labor: Firm-Level Evidence. *The Quarterly Journal of Economics*, *117*(1), 339-376. https://doi.org/10.1162/003355302753399526

Brynjolfsson, E., Jin, W., & McElheran, K. (2021). The power of prediction: Predictive analytics, workplace complements, and business performance. *Business Economics*, *56*(4), 217-239. https://doi.org/10.1057/s11369-021-00224-5

Buckman, J., Hashim, M. J., Woutersen, T., & Bockstedt, J. (2018). *Fool me twice: An analysis of repeat data breaches within firms*. SSRN. http://dx.doi.org/10.2139/ssrn.3258599

Callaway, B., & Sant'Anna, P. H. C. (2021). Difference-in-differences with multiple time periods. *Journal of Econometrics*, *225*(2), 200-230. https://doi.org/10.1016/j.jeconom.2020.12.001

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Deming, D., & Kahn, L. B. (2018). Skill requirements across firms and labor markets: Evidence from job postings for professionals. *Journal of Labor Economics*, *36*(S1), S337-S369. https://doi.org/10.1086/694106

Executive Order No. 13800, 82 Fed. Reg. 22391 (May 16, 2017). https://www.federalregister.gov/d/2017-10004

Executive Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021). https://www.federalregister.gov/d/2021-10460

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of timing? *Management Science*, *68*(10), 7298-7322. https://doi.org/10.1287/mnsc.2021.4264

Freyaldenhoven, S., Hansen, C., & Shapiro, J. M. (2019). Pre-event trends in the panel event-study design. *American Economic Review*, *109*(9), 3307-3338. https://doi.org/10.1257/aer.20180609

Goodman-Bacon, A. (2021). Difference-In-Differences with Variation in Treatment Timing. *Journal of Econometrics*, *225*(2), 254-277. https://doi.org/10.1016/j.jeconom.2021.03.014

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST cybersecurity framework via the Gordon-Loeb model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85-105. https://doi.org/10.1509/jm.16.0124

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaspersky Lab. (2018). *Survey finds that 84% of CISOs in North America believe cybersecurity breaches are inevitable.* https://usa.kaspersky.com/about/press-releases/2018_survey-finds-that-84-of-cisos-in-north-america-believe-cybersecurity-breaches-are-inevitable

Kelly, C. (2005). Data security: A new concern for PR practitioners. *Public Relations Quarterly*, *50*(2), 25-26.

Kim, B., Johnson, K., & Park, S.-Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1). https://doi.org/10.1080/23311975.2017.1354525

Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly*, *47*(1), 317-342. https://doi.org/10.25300/MISQ/2022/15713

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787. https://doi.org/10.1080/07421222.2020.1790190

Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44-59. https://doi.org/10.1177/1094670510383409

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, *31*(4), 829-848. https://doi.org/10.1007/s12525-021-00490-3

Ponemon Institute. (2020). *The economic value of prevention in the cybersecurity lifecycle* (Ponemon Institute research report). https://www.ponemon.org/research/ponemon-library/security/the-economic-value-of-prevention-in-the-cybersecurity-lifecycle.html

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, *33*(3), 227-265. https://doi.org/10.2308/isys-52379

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74-104. https://doi.org/10.1111/jels.12035

Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. *Strategy Science*, *5*(2), 117-142. https://doi.org/10.1287/stsc.2020.0106

Słoczyński, T. (2022). Interpreting OLS estimands when treatment effects are heterogeneous: Smaller groups get larger weights. *The Review of Economics and Statistics*, *104*(3), 501-509. https://doi.org/10.1162/rest_a_00953

Sun, L., & Abraham, S. (2021). Estimating dynamic treatment effects in event studies with heterogeneous treatment effects. *Journal of Econometrics*, *225*(2), 175-199. https://doi.org/10.1016/j.jeconom.2020.09.006

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417-440. https://doi.org/10.1111/lsi.12303

Toth, P. (2018, October 4). Cybersecurity starts with your employees. *National Institute of Standards and Technology—Manufacturing Innovation Blog*. https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-starts-your-employees

Turjeman, D., & Feinberg, F. M. (2024). When the data are out: Measuring behavioral changes following a data breach. *Marketing Science*, *43*(2), 440-461 https://doi.org/10.1287/mksc.2019.0208

Vaaler, P. M., & Greenwood, B. (2023). Do US state breach notification laws decrease firm data breaches? *Review of Law & Economics*. https://doi.org/10.1515/rle-2023-0038

Woods, D. W., Böhme, R., Wolff, J., & Schwarcz, D. (2023). Lessons lost: Incident response in the age of cyber insurance and breach attorneys. In *Proceedings of the 32nd USENIX Security Symposium* (pp. 2259-2273). https://www.usenix.org/system/files/usenixsecurity23-woods.pdf

Woods, D. W., & Ceross, A. (2021). Blessed are the lawyers, for they shall inherit cybersecurity. In *Proceedings of the 2021 New Security Paradigms Workshop* https://doi.org/10.1145/3498891.3501257

About the Authors

Sarah Bana (ORCID ID: 0000-0002-6761-4862) is an assistant professor of management science at Chapman University. She is also a Digital Fellow at the Stanford Digital Economy Lab. Dr. Bana's research explores how new technologies and data reshape the skills and activities of workers and firms. Her research has been published in outlets such as *Journal of Econometrics, Journal of Policy Analysis and Management, and Sloan Management Review*, and featured by the BBC Business Daily. Dr. Bana's research has been funded by the Russell Sage Foundation. She received her Ph.D. in economics at the University of California, Santa Barbara.

Erik Brynjolfsson (ORCID ID: 0000-0002-8031-6990) is a professor, author, and inventor. At Stanford, he is a professor at the Institute for Human-Centered AI (HAI) and director of the Digital Economy Lab, with positions at SIEPR, the Economics Department, and the Graduate School of Business. His research and speaking focus on the economics of AI and digital technologies, including their effects on productivity, business strategy, and the future of work. Brynjolfsson is a best-selling author of several books including *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.* He has written over 200 academic articles and is one of the most widely cited researchers on the economics of AI. Brynjolfsson holds five patents and is the co-founder of Workhelix, Inc, which helps companies identify opportunities for generative AI.

Wang Jin (ORCID ID: 0000-0003-4813-2507) is a research scientist at the Stanford Digital Economy Lab and a Digital Fellow at the IDE, Sloan School of Management. His research focuses on the impact of emerging technologies and organizational practices on firms' productivity, employment, innovation, and future of work. His work has been published in *Management Science*, *Harvard Business Review*, and *Business Economics*. Wang Jin received his Ph.D. in economics from Clark University.

Sebastian Steffen (ORCID ID: 0000-0002-3262-290X) is an assistant professor in the Business Analytics Department at the Carroll School of Management at Boston College. He is also a Digital Fellow with the Stanford Digital Economy Lab (S-DEL) and the MIT Initiative on the Digital Economy (IDE). His research focuses on how technologies transform businesses and society and how they impact the value of human capital and the future of work. Sebastian received his Ph.D. in Management Science from the MIT Sloan School of Management and his BA in Economics from Princeton University.

Xiupeng Wang (ORCID ID: 0000-0002-0486-7707) is on the faculty at the D'Amore-McKim School of Business at Northeastern University and a Digital Fellow at the Stanford Digital Economy Lab. Dr. Wang's research primarily focuses on the impact of emerging information technologies on firms and the labor market. Dr. Wang received his Ph.D. in economics from the University of Connecticut and did postdoc research at MIT, Stanford University, and Boston University. He is also a senior research associate at the Harvard Labor and Worklife Program.

Appendix

Definitions of Cybersecurity, PR, and Legal SOC Occupations

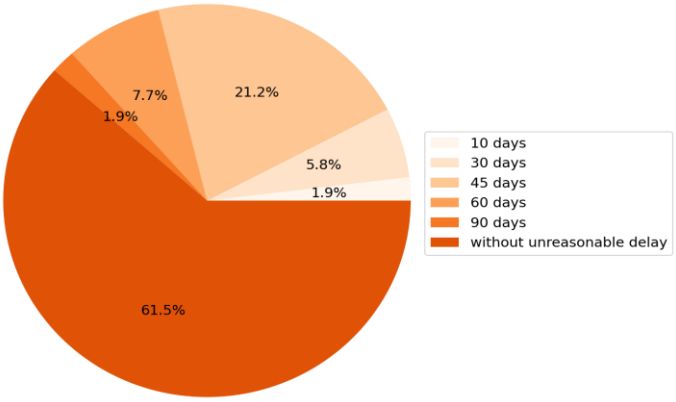
Our paper defines three categories of jobs relevant to data breaches: cybersecurity, PR, and legal. To select the job postings that fall into these categories, we relied on the posting's Standard Occupation Classification (SOC) code. Table A1 provides a detailed list of the specific occupations included in each category. In cases where the SOC code changed between the 2010 and 2018 classifications, we note the year associated with the code.

Table A1. Definitions of Cybersecurity, PR, and Legal SOC Occupations

SOC code	SOC name	Notes
15-1120	Computer and Information Analysts	Cybersecurity; 2010 Code
15-1121	Computer Systems Analysts	Cybersecurity; 2010 Code
15-1122	Information Security Analysts	Cybersecurity; 2010 Code
15-1140	Database and Systems Administrators and Network Architects	Cybersecurity; 2010 Code
15-1141	Database Administrators	Cybersecurity; 2010 Code
15-1142	Network and Computer Systems Administrators	Cybersecurity; 2010 Code
15-1143	Computer Network Architects	Cybersecurity; 2010 Code
15-1152	Computer Network Support Specialists	Cybersecurity; 2010 Code
15-1210	Computer and Information Analysts	Cybersecurity; 2018 Code
15-1211	Computer Systems Analysts	Cybersecurity; 2018 Code
15-1212	Information Security Analysts	Cybersecurity; 2018 Code
15-1231	Computer Network Support Specialists	Cybersecurity; 2018 Code
15-1240	Database and Network Administrators and Architects	Cybersecurity; 2018 Code
15-1241	Computer Network Architects	Cybersecurity; 2018 Code
15-1244	Network and Computer Systems Administrators	Cybersecurity; 2018 Code
15-1245	Database Administrators and Architects	Cybersecurity; 2018 Code
11-2030	Public Relations and Fundraising Managers	PR
11-2032	Public Relations Managers	PR
27-3030	Public Relations Specialists	PR
27-3031	Public Relations Specialists	PR
23-1011	Lawyers	Legal
23-2011	Paralegals and Legal Assistants	Legal

Data Breach Notification Laws and Data Breach Announcement Timing

As discussed in the Empirical Methods section, data breach notification laws in most states require firms to report such events without reasonable delay or within 30 to 60 days of noticing a breach of individual customer data. Therefore, the treatment time was not sharply identified at month zero, as there could have been strategic timing decisions by firms on when to announce breach events (Foerderer & Schuetz, 2022). We used the data breach announcement date as the treatment date for our baseline specification. While this is likely neither the exact date of the breach nor the date on which the firm noticed the breach, we consider it to be the most reasonable date available. However, in order to reduce noise due to the ambiguity in the treatment timing, we also tested specifications that dropped the observations from Quarter 0 (Months 0, -1, and -2) and present these results in Table A2. The results are largely consistent with our baseline results from Column 1 in Tables 2, 3, and 4.



Note: Figure derived from Perkins Coie Security Breach Notification data—Revised June 2020, available at https://www.perkinscoie.com/en/newsinsights/security-breach-notification-chart.html. About 60% of US states require breached firms to notify the public as soon as they realize that they were breached. In total, 98% of all US states require firms to notify the public no longer than 60 days after suffering a data breach.

Figure A1. Timely Notification Requirements by States' Data Breach Notification Laws

While our analysis is predicated on the change that occurred before and after the breach, it may be the case that firms strategically disclosed their breach and hired prior to the breach disclosure. To mitigate the concern that strategic disclosure may have affected our results, we estimated the main regression, excluding Quarter 0 while including an additional preceding quarter, e.g., Quarter -4—i.e., we excluded Months -2, -1, and 0 from our estimation. These were the months most likely to be affected by strategic disclosure, as discussed above.

Table A2. Effect of Data Breaches on Hiring (Excluding Quarter 0)

Occupations	**Cybersecurity**	**PR**	**Legal**
Variables	**(1)**	**(2)**	**(3)**
	Full sample	**Full sample**	**Full sample**
After × Breached	0.024*** (0.005)	0.011*** (0.003)	0.008** (0.003)
R-squared	0.308	0.172	0.245
# of firms	89,121	89,121	89,121

Note: All results are based on the full analytic sample, similar to Column 1 of Tables 2, 3, and 4. Each column estimates the difference-in-differences specification outlined in Equation (1) in the manuscript. Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Alternative Time Window

Our main analysis used a window of four quarters before and after the data breach. However, one concern is that this extended window may not have effectively captured the transient nature of the breach's impact. Moreover, a longer time window may increase the probability of confounding factors that could be a source of bias. We therefore reestimated our main specification, restricting the sample period to only two quarters before and after the breach. The results are largely consistent with our baseline results from Column 1 of Tables 2, 3, and 4.

Table A3. Effect of Data Breaches on Hiring (Two Quarters Before and After)

Occupations	**Cybersecurity**	**PR**	**Legal**
Variables	**(1)**	**(2)**	**(3)**
	Full sample	**Full sample**	**Full sample**
After × Breached	0.019*** (0.005)	0.010*** (0.004)	0.004 (0.004)
R-squared	0.307	0.171	0.244
# of firms	89,063	89,063	89,063

Note: All results are based on the full analytic sample, similar to Column 1 of Tables 2, 3, and 4 with one key difference: we focused on a shorter time window (i.e., two quarters before and after the data breach events). Each column estimates the difference-in-differences specification outlined in Equation (1). Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Alternative Model Specification

Linear probability models have two primary limitations: They can produce predicted probabilities outside of the zero-one range, and they possess constant marginal effects. As a result, a logit model may be more conducive when the dependent variable is binary, as in our case. We estimated the main regression in Column 1 of Tables 2, 3, and 4, replacing the linear probability model with a logit model. Due to computational limitations and the incidental parameter problems associated with nonlinear models, we estimated the regression with only firm fixed effects. The results are displayed in Table A4.

Table A4. Effect of Data Breaches on Hiring (Logit Models)

Occupations	Cybersecurity	PR	Legal
Variables	(1)	(2)	(3)
	Full sample	Full sample	Full sample
After × Breached	0.367***	0.238***	0.238***
	(0.039)	(0.050)	(0.054)
# of firms	59,370	32,521	26,214

Note: Columns 1, 2, and 3 estimate the two-period difference-in-differences specification outlined in Equation (1). Each cell reports the coefficients of the independent variable from the Logit model. Only firm-fixed effects are included in the specifications because of computational limitations and the incidental parameter problem associated with fixed effects. Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Quarterly Dynamics with Propensity Score Matching

Although our identification strategy exploits the fact that the timing of the data breach events is largely unanticipated by affected firms, post-event labor demand may have been driven by other firm-level characteristics prior to the data breaches, such as firm size or firms' prior hiring for cybersecurity and other personnel, which could have led to biased estimates. We thus performed propensity score matching to construct a sample consisting of control and treatment firms that are relatively more similar, based on pre-data-breach firm-level observables. More specifically, we matched each firm using their cumulative number of job postings (as a proxy for firm size), the cumulative number of job postings for cybersecurity, PR, and legal talent in the 12 months prior, as well as the industry of the firms. We matched the treatment and control groups using the nearest-neighbor matching method and imposed common support with five neighbors and a 0.001 caliper.[11] Using the matched sample, we reestimated our baseline specification of quarterly dynamics. We found consistent and robust results similar to the ones reported in Figures 1, 2, and 3.

Table A5. Quarterly Dynamics with Matched Sample sing Propensity Score Matching

Occupations	Cybersecurity	Public Relations	Legal
Variables	(1) Matched sample	(2) Matched sample	(3) Matched sample
Quarter -3	-0.009	0.005	-0.005
	(0.008)	(0.006)	(0.006)
Quarter -2	-0.009	-0.003	-0.000
	(0.007)	(0.006)	(0.005)
Quarter 0	0.002	0.008	0.005
	(0.007)	(0.005)	(0.005)
Quarter +1	0.006	0.012**	-0.008
	(0.008)	(0.006)	(0.006)
Quarter +2	0.025***	0.010*	0.012**
	(0.009)	(0.006)	(0.006)
Quarter +3	0.010	0.002	0.003
	(0.009)	(0.006)	(0.006)
Quarter +4	0.012	0.010	0.004
	(0.009)	(0.006)	(0.006)
Observations	610,932	610,932	610,932
R-squared	0.424	0.282	0.338
# of firms	5,534	5,534	5,534
Mean(Y)	0.164	0.047	0.047

Note: The results are based on the matched sample. The outcome variables for Columns 1-3 are the indicators for firms that, respectively, posted jobs for cybersecurity, public relations, and legal occupations. Quarter -1 is the benchmark period. Firm, industry, time, and pair fixed effects were controlled for in the specification. Robust standard errors are reported in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

[11] Robustness checks using different numbers of nearest neighbors generated similar results. These results are available upon request.

Placebo Test of Non-Relevant Occupations

Though we identified significant effects throughout the manuscript, one potential concern may be that these identified demand increases may have coincided with other shocks to the firm that were not a function of a data breach. To address this concern, we replicated our main table for occupations not relevant to a data breach, i.e. any occupation not defined in Table A1 above.

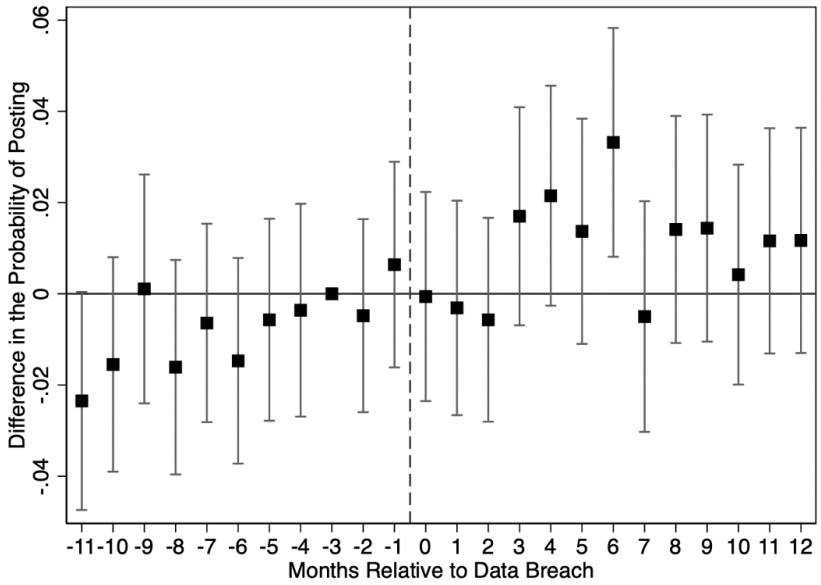
Table A6. Effect of Data Breaches on Hiring for Non-Relevant Occupations

Models	**Probability**			**Counts**	
Variables	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
	Full sample	**Matched sample**	**Matched sample Sun & Abraham**	**Full sample**	**Full sample Poisson**
After × Breached	-0.008 (0.007)	0.002 (0.009)	0.003 (0.009)	16.45 (10.35)	0.978 (0.081)
R-squared	0.311	0.346	0.352	0.383	-
# of firms	89,121	5,077	5077	89,121	89,043

Note: Results in Columns 1, 4, and 5 are based on the full sample. Results in Columns 2 and 4 are based on the matched sample. Each column estimates the difference-in-differences specification outlined in Equation (1) while Column 3 further employs the S&A estimator. Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

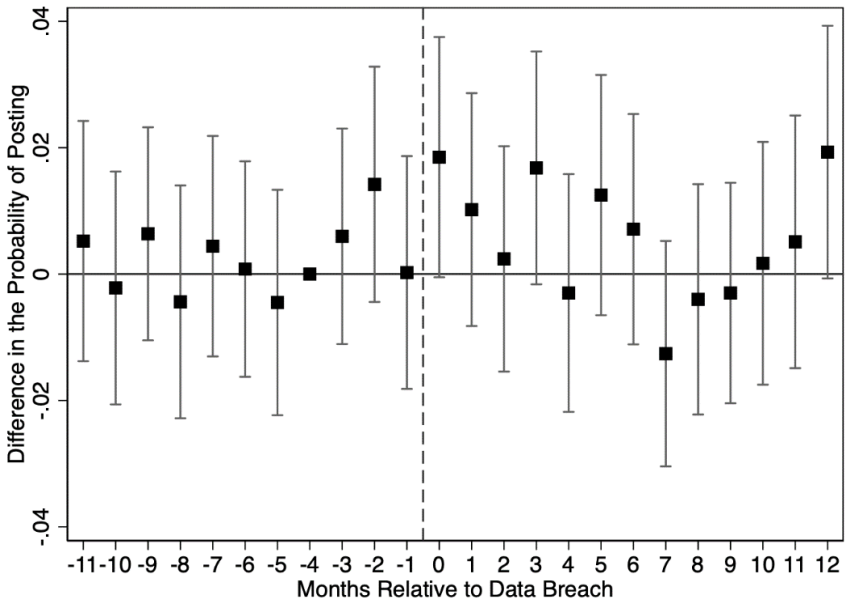
Monthly Dynamics of Firm's Hiring in Response to Data Breaches

To further assess the monthly dynamics of firms' hiring in response to data breaches, we estimated a model with monthly indicators with a propensity score matched sample.



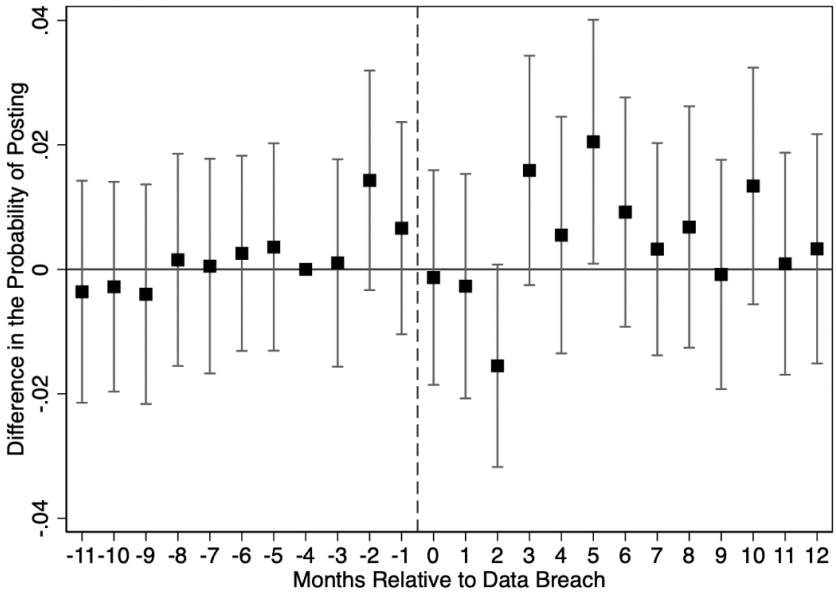
Note: Figure A2 displays the parallel trends test described in the Empirical Methods section, using the monthly coefficients on the matched sample. Month -3 is the omitted category. The reported 95% confidence intervals use standard errors clustered at the firm level.

Figure A2. Monthly Dynamic for Cybersecurity Hiring



Note: Figure A3 displays the parallel trends test described in the Empirical Methods section, using the monthly coefficients on the matched sample. Month -3 is the omitted category. The reported 95% confidence intervals use standard errors clustered at the firm level.

Figure A3. Monthly Dynamic for PR Hiring



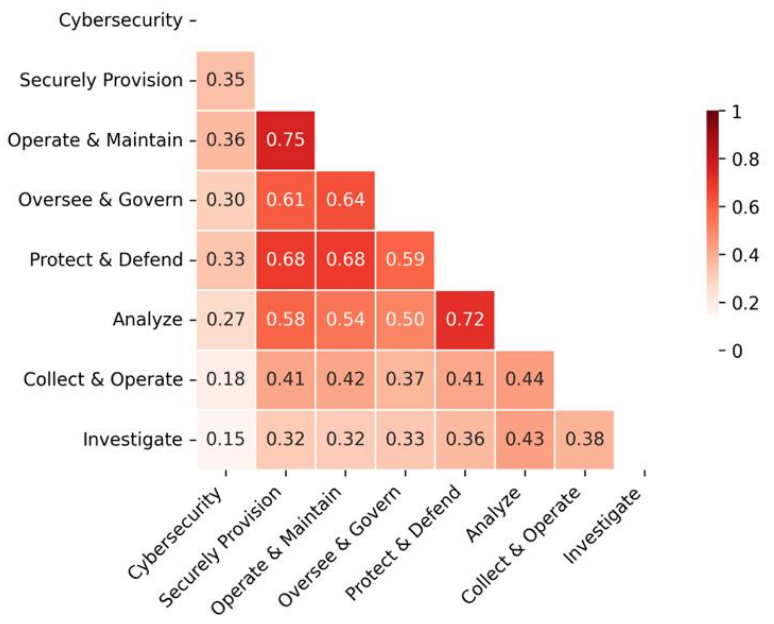
Note: Figure A4 displays the parallel trends test described in the Empirical Methods section, using the monthly coefficients on the matched sample. Month -3 is the omitted category. The reported 95% confidence intervals use standard errors clustered at the firm level

Figure A4. Monthly Dynamic for Legal Hiring

Correlation Between NICE Categories and Cybersecurity Occupations

Figure A5 shows the correlation between the cybersecurity-related indicator variables in our study: our definition of cybersecurity occupations, which is an occupation-based measure, and the Lightcast correspondence to the seven NICE categories. The cybersecurity occupation measure, which includes IT and computer networking-related occupations, is positively correlated with the NICE-based measures of cybersecurity functions, suggesting that the cybersecurity-related skills captured by the NICE framework cover a more targeted range of cybersecurity-related functions.

Moreover, while indicator variables for NICE categories are highly correlated with one another—for example, the Securely Provision and Operate & Maintain functions show a correlation coefficient of 0.75—others are less correlated, indicating meaningful differences across these functions. The findings thus emphasize the demand heterogeneity across occupations and skills and highlight the value of the NICE categories as an alternative cybersecurity definition for identifying granular yet distinctive hiring responses.



Note: This heatmap visualizes the correlation coefficients of cybersecurity variables and NICE indicators, derived from the estimation sample.

Figure A5. Heatmap of Cybersecurity Variables

Effect Heterogeneity of Data Breaches by NICE Cybersecurity Functions

The relative effect size (measured by the coefficient divided by the dependent variable mean) is greatest for "Oversee & Govern" at 168% (0.021/0.013). This is consistent with firms hiring workers to manage and develop strategies for cybersecurity work. While CIOs and CTOs fall into this domain, this also includes non-executive workers, such as IT project auditors, project managers, program managers, and cyber policy and strategy planners. The second largest effect appears for "Protect & Defend"—roles that identify, analyze, and mitigate threats to IT systems and networks, such as vulnerability assessment analysts and cyber-defense analysts, among others. This effect demonstrates that firms that experience breaches respond substantively and in a targeted manner to incidents by strategically improving relevant infrastructure and/or assessing their systems and networks to understand their vulnerabilities. In contrast, we did not observe firms seeking cybersecurity roles that fall into the "Collect & Operate" or "Investigate" categories. "Collect & Operate" involves providing specialized denial and deception operations.

Table A7. Effect Heterogeneity by Cybersecurity Functions (Cyber Breaches Only)							
Categories	**Securely Provision**	**Operate & Maintain**	**Oversee & Govern**	**Protect & Defend**	**Analyze**	**Collect & Operate**	**Investigate**
Variables	**(1) Full sample**	**(2) Full sample**	**(3) Full sample**	**(4) Full sample**	**(5) Full sample**	**(6) Full sample**	**(7) Full sample**
After × Breached	0.019***	0.021***	0.021***	0.018***	0.011***	0.006**	0.003
	(0.005)	(0.005)	(0.005)	(0.005)	(0.004)	(0.003)	(0.002)
R-squared	0.136	0.137	0.116	0.120	0.102	0.093	0.082
# of firms	88,078	88,078	88,078	88,078	88,078	88,078	88,078
Mean(*Y*)	0.015	0.017	0.013	0.012	0.007	0.004	0.002

Note: Results are based on the full sample with cyber-related data breaches only since NICE is a cybersecurity workforce framework. Each column estimates the difference-in-differences specification outlined in Equation (1). The dependent variables are binary indicators that equal one for firms posting any job ads that correspond to each category from the NICE Cybersecurity framework. Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.

Matching Lightcast Hiring Data with PRC Data Breach Events

Since the PRC and Lightcast databases do not share a common firm identifier, we took a multistep approach to merge the two databases. Specifically, we first cleaned and standardized the firm name strings in both databases. Next, we used a combination of name and address fuzzy matching to construct a bridge between the PRC and Lightcast data. After algorithmic matching, we manually validated and checked all possible high-quality matches to further increase the match rate. Overall, we identified and matched over 50% of organizations from the PRC data in the Lightcast data. We further required that all organizations had at least 100 job postings in the Lightcast data (i.e., 2010 - 2020) to ensure sufficient quality of the job posting data, though our results are robust to different cutoffs. Overall, our main sample contained a total of over 87,000 organizations and over 1,400 data breach events. Many matched organizations in the PRC data were smaller local businesses (e.g., local clinics) and were hence dropped due to the 100-job posting cutoff we impose. On average, organizations in our sample had 12 job postings per month, with about 0.32 of them related to cybersecurity occupations in each month.

Wage Bill Estimation

To better understand the economic magnitude of these hiring responses, we estimated the implied wage bill increases in monetary terms. Since reliable wage information is often absent from job postings (Batra et al. 2023), we used average, occupation-level annual wages from the Bureau of Labor Statistics' Occupational Employment and Wage Statistics (OEWS) along with the number of job postings in the related occupations to calculate firms' implied additional wage bills that they intended to spend on hiring. We estimated Equation (1), our main regression specification, with the wage bills associated with cybersecurity, PR, and legal hiring. In addition, we also performed the specification on the total wage bill, which combined the three categories.

Table A8. Effect of Data Breach on Wage Bill				
Occupations	**Total wage bill**	**Cybersecurity**	**PR**	**Legal**
Variables	**(1) Full sample**	**(2) Full sample**	**(3) Full sample**	**(4) Full sample**
After × Breached	61,961***	52,010***	1,965	7,986***
	(14,701)	(13,192)	(1,836)	(1,883)
R-squared	0.880	0.895	0.324	0.469
# of firms	89,121	89,121	89,121	89,121

Note: All results are based on the full analytic sample, similar to the one used in Column 1 of Tables 2, 3, and 4 with the dependent variable as the imputed wage bill the firms intended to spend on additional hiring. Each column estimates the difference-in-differences specification outlined in Equation (1). Standard errors are clustered at the firm level in parentheses. *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.