Treating the Symptoms or the Cause: Symbolic and Substantive Talent Acquisition in Response to Data Breaches

Sarah Bana [1] Erik Brynjolfsson [1] Wang Jin [2] Sebastian Steffen [2] Xiupeng Wang [3]

[1]Stanford University [2]MIT [3]Skidmore College

Research Questions

- Little is known about the effects of data breaches on firms post-incident human capital investments.
- Do firms react to data breaches by investing in cybersecurity talent or are they more likely to invest in talent that helps save their public image or tackle subsequent legal issues?
- Does public scrutiny affect firm's choice of treatment: substantive vs. symbolic?

Data Breaches Are Costly

$180
Per record cost of personally identifiable information

287
Average number of days to identify and contain a data breach

$4.62m
Average total cost of a ransomware breach

Source: IBM Security: Cost of a Data Breach Report 2021

Hypotheses

- **Hypothesis 1** Firms adopt substantive measures and increase their demand for cybersecurity workers to treat the root cause of a data breach;
- **Hypothesis 2** Firms adopt symbolic measures and increase their demand for PR and Legal workers to treat the symptoms of a data breach;
- **Hypothesis 3** Firms that experience sharply elevated public scrutiny will increase substantive adoption relatively more than symbolic adoption.

Data & Methodology

- Job postings: **Burning Glass Technologies**
- Data breach events: **Privacy Rights Clearinghouse**
- Media attention: **The MIT Media Cloud project**
- Public attention: **Google Trends**

$$Jobs_{i,j,t} = \beta_0 + \beta_D D_{i,t} + \lambda_i + \lambda_y + \lambda_{m,j} + \varepsilon_{i,j,t}$$

- $Jobs_{ijt}$: indicator for whether the firm posts job vacancies for a certain occupation;
- $D_{i,t}$: indicator for whether the observed month is after the data breach event.

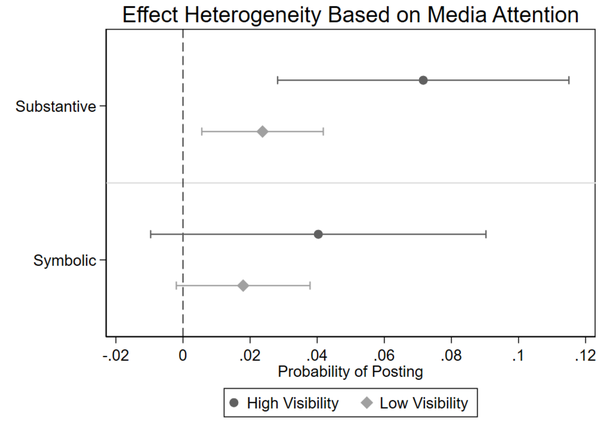
Results: Effect on Talent Demand

	Substantive Adoption Cybersecurity		Symbolic Adoption PR and Legal		Not Relevant Other Occupations
	(1) Pre/Post	(2) Quarterly	(3) Pre/Post	(4) Quarterly	(5) Pre/Post
Post Breach	0.018***		0.0174***		0.010
	(0.005)		(0.00552)		(0.006)
Quarter (-1)		0.001		0.00345	
		(0.006)		(0.00655)	
Quarter (+1)		0.012*		0.00942	
		(0.007)		(0.00708)	
Quarter (+2)		0.027***		0.0314***	
		(0.008)		(0.00786)	
Firms	89,145	89,145	89146	89146	89146
R-squared	0.291	0.291	0.233	0.233	0.300

Standard errors clustered at the firm level in parentheses.
*** p<0.01, ** p<0.05, * p<0.1

- Breached firms take both substantive and symbolic measures after a data breach.
- No effect on firms' demand on non-relevant talents.

Effect on Talent Acquisition by Media Attention



- Identify large jumps in firms' media attention around data breach events.
- Similar results for different cutoffs of high vs. low attention.
- Public attention with Google Trends gives similar results.

Conclusion

- Breached firms demand more cybersecurity than non-breached firms.
- Hiring effect on the breached firms is relatively small compared to the severity of these types of cyberattacks.
- Firms are also more likely to increase their demand for legal and public relations talents after data breaches.
- Firms with increased public scrutiny are more likely to respond to data breaches by acquiring cybersecurity talent, but less so for legal and PR talent.
- $\Rightarrow$ Public scrutiny can serve as effective mechanism to align firms' incentives with public and internalize externalities.