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

¹Stanford University ²MIT ³Skidmore 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

$180 287 $4.62m
Per record cost of Average number of days to identify and contain a Average total cost of a personally identifiable data breach data 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

\[ jobs_{i,j,t} = \beta_0 + \beta_mD_{i,t} + \lambda_i + \lambda_y + \lambda_{m,j} + \varepsilon_{i,j,t} \]

\( jobs_{i,j,t} \): 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

<table>
<thead>
<tr>
<th></th>
<th>Substantive Adoption</th>
<th>Symbolic Adoption</th>
<th>Not Relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pre/Post Quarterly</td>
<td>Pre/Post Quarterly</td>
<td>Pre/Post</td>
</tr>
<tr>
<td>Pre/Post Breach</td>
<td>0.018*** (0.005)</td>
<td>0.0174*** (0.0052)</td>
<td>0.010 (0.006)</td>
</tr>
<tr>
<td>Quarter (-1)</td>
<td>0.001 (0.006)</td>
<td>0.00345 (0.0055)</td>
<td></td>
</tr>
<tr>
<td>Quarter (+1)</td>
<td>0.012* (0.007)</td>
<td>0.00942 (0.00708)</td>
<td></td>
</tr>
<tr>
<td>Quarter (+2)</td>
<td>0.027*** (0.008)</td>
<td>0.0314*** (0.00786)</td>
<td></td>
</tr>
<tr>
<td>Firms</td>
<td>89.145</td>
<td>89.145</td>
<td>89.146</td>
</tr>
<tr>
<td>R-squared</td>
<td>0.291 0.291</td>
<td>0.233 0.233</td>
<td>0.200</td>
</tr>
</tbody>
</table>

Standard errors clustered at the firm level in parentheses.

• 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.
• Public scrutiny can serve as effective mechanism to align firms’ incentives with public and internalize externalities.

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.
• Public scrutiny can serve as effective mechanism to align firms’ incentives with public and internalize externalities.