Resource-based Perspective on Slack and Data Breach

Emergent Research Forum (ERF) Papers

Qian Wang
Department of Management and Marketing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, PR China
qian.mp.wang@connect.polyu.hk

E.W.T. Ngai
Department of Management and Marketing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, PR China
eric.ngai@polyu.edu.hk

Abstract

In the last couple of years, data breach has become a top concern for enterprises and consumers. Resource-based view (RBV) suggests that firms are proactive, and the low marginal cost of slack will motivate and enable firms to have new activities by redeploying the stocked excess resources to achieve competitive advantages. Based on the RBV, this study explores both the input and opportunity effectiveness of slack on data breach risk. In terms of the former, we firstly test the association between human resource (HR) slack and data breach risk; in terms of the later, we further investigate how the interaction of HR slack and financial slack can impact data breach risk. Besides, from firm external lens, we also test whether the influence of HR slack on data breach risk is contingent upon external environments.

Keywords

Data breach risk, human resource slack, financial slack, industry environments, internal and external risk, resource-based view.

Introduction

Data, as an organization’s valuable asset, can create efficiencies, eliminate waste, and increase the required access to information. However, data can also foster new threats for breaches (Hovav and D’Arcy 2003). Presently, a combination of infinite high-profile data breaches and a growing number of related regulatory requirements (e.g., FTC Act, GLB, and HIPAA) has pushed data breach controls to be listed at the forefront of the strategic agenda of most firms (Angst et al. 2017).

Over the last two decades, security scholars have realized that organizational and managerial factors, in addition to technological factors, can play crucial roles in influencing IT security performance (Vermeulen and Von Solms 2002). Thus, several recent works have detected presumed organizational determinants for data breach risks, such as information technology governance, information security investment, and organization culture. We aim to contribute to this discourse from a novel perspective of resource slack. Specifically, slack can play a role through two paths, namely, excess inputs and unexploited opportunities (Nohria and Gulati 1996). In our study, in the context of IT security, we explore the input effectiveness of slack via human resource (HR) slack and the opportunity effectiveness of slack via financial slack.

According to resource-based views (RBV), firms are proactive, and managers decide strategically by redeploying excess resources to achieve competitive advantages (Hart 1995). The excess resources have the advantages that, when strategically redeployed, they can provide services at very low or even (near-) zero marginal cost, and therefore, to engender endogenous innovation and growth, managers commonly take slack as a most crucial inducement to start new activities (Pitelis 2007).

In the same vein, when firms stock HR slacks, the potential advantages of the excess HRs will enable and motivate managers to redeploy them. However, HR slack is a most representative type of absorbed slack (Mishina et al. 2004). They are hard to be redeployed, and the time frame over which these resources can be redeployed is long (Voss et al. 2008). The structural difficulty accompanies shifting intra-firm for HRs
anticipates the possibility of employee maladjustments or unawareness in terms of their IT knowledge and operations, thereby increasing data breach risks (Colwill 2009).

Notably, a novelty of our study is that we distinguish between internal and external risks in terms of investigating the input effectiveness of HR slack. These internal and external data breaches differ significantly in their causes and controls. One organizational factor can provide an effective security layer against outsiders while lead to disastrous results at managing insider risks (Colwill 2009). The issue on using empirical research can be a plausible explanation for the mixed empirical results in prior studies which focus on the link between IT investment and data breach risks (e.g., Angst et al. 2017; Kwon and Johnson 2014).

To further explore the slack opportunity effectiveness in the context of IT security, we also examine the effect of the interaction of HR and financial slack on data breach risk. This interaction effect occurs because the resulting IT maladjustment incurred by insiders and other weaknesses of the IT systems can be better buffered through additional security education or other IT investments supported by more financial slack (Colwill 2009). Such an action can intervene with the effect of HR slack on data breach risk.

Moreover, we also explore the moderating effects from firm external lens by examining how the interaction of HR slack and external environments can affect data breach risk. Under various environments, the likelihood for managers to develop proactive strategies based on resources significantly differ (Aragón-Correa and Sharma 2003). Thus, the requirements of firms to strategically redeploy their excess resources are distinct across environments (Hart 1995), thereby moderating the influence of slack on data breach risk.

In a nutshell, this paper is aimed at examining the relationships among HR slack, data breach risk, and two moderators of financial slack and external environments by considering the following principal questions: “How can HR slack influence data breach risk?” and “Can financial slack or industry environment intervene on this influence?”. Addressing these research questions is helpful in providing linkage between organizational and IS security research on slack theory and reminding managers to balance the advantages (low marginal cost) and disadvantages (higher IT security risks) of HR slacks when strategically redeploy them.

**Theory and Hypotheses**

A “resource-based view” serves as the theoretical foundation of our analysis. RBV theorists (e.g., Pitelis 2007) suggest that, since the excess resources can provide new services at very low or (near-) zero marginal cost, the pool of surplus resources can serve as a crucial internal inducement for firms to start new activities to achieve economic soundness. Based on the RBV, we consider firm endogenous (input and opportunity effect of slack) and exogenous (external environment) factors in investigating data breach risk. The approach to classify data breaches into internal and external categories is based on the parties (i.e., insiders and outsiders) that caused the leakage. Figure 1 demonstrates the overall research framework.

**Figure 1. Research framework**

HR slack is a highly representative type of absorbed slack (Mishina et al. 2004). Human capabilities are closely tied up with the current operations of an organization. Owing to this rationale, the IT knowledge and skills of an employee are prone to being rooted to a specific task or position. In such a case, matching the employee with a new deployment becomes difficult, thereby increasing the potential for an internal data breach (Colwill 2009). Moreover, the RBV also indicates that holding HRs is costly (Hart 1995). Excessive
idle labor resources will indirectly reduce other resources that would have been used for the firms’ proactive IT investment and maintenance, which is powerful at thwarting external hackers. The abovementioned evidence leads to the following hypotheses.

**H1a**: HR slack will positively influence corporate internal data breach risk.

**H1b**: HR slack will positively influence corporate external data breach risk.

**H1c**: HR slack will positively influence corporate universal data breach risk.

Excess financial slack can support security education and awareness programs for insiders and sustain IT system updates against malicious outsiders (Colwill 2009). Following this rationale, if a firm stocks more financial slack when it strategically redeployed its excess HRs, the resulting IT-related problems will be alleviated. Thus, we hypothesize as follows:

**H2**: Increased financial slack will weaken the positive influence of HR slack on data breach risk.

Under various external environments, the willingness of managers to employ firm resources to proactively react to contingencies varies significantly (Aragón-Correa and Sharma 2003). We consider two widely used environmental dimensions, namely, dynamism and complexity, to assess the general external environment of a firm. “Dynamism” represents the rate of change in innovation or unpredictability of the actions in the environment, whereas “complexity” theoretically means the proliferation and diversity of factors in that environment (Duncan 1972).

Instability in a dynamic environment widens the opportunities to managers for proactive strategies; such managers enforce further innovative strategies (Miles et al. 1978). Meanwhile, in complex industries, managers prefer minimal adjustments and are not willing to use their resources to develop proactive strategies because of the less mutual awareness and industry norm (Aragón-Correa and Sharma 2003). Therefore, dynamism may increase the frequency for firms to strategically redeploy their HR slack, whereas complexity may reduce this frequency. By incorporating the arguments in **H1** and the abovementioned evidence, we suggest the following hypotheses.

**H3a**: A high environmental dynamism will strengthen the positive influence of HR slack on data breach risk.

**H3b**: A high environmental complexity will weaken the positive influence of HR slack on data breach risk.

### Data and Variables

**Data Description**

The data that we used are from two public sources, namely, Privacy Rights Clearinghouse (privacyrights.org) and COMPUSTAT. Figure 2 illustrates our data collection processes.

![Data collection procedures](image)

**Variable Descriptions**

**Dependent Variables**

Data breach (BREACH)/external data breach (BREACH_EXT)/internal data breach (BREACH_IN): an indicator variable equal to 1 if a firm has a reported external data breach/internal data breach/data breach in the current fiscal year, or 0 otherwise.

**Independent Variables**

HR slack (HR_SLACK): we calculate the HR slack by using the following equation:
Human resource slack = \frac{\text{Firm employees}}{\text{Firm sales}} - \frac{\text{Industry employees}}{\text{Industry sales}}

\textbf{Moderators}

- Financial Slack (FIN\_SLACK): we construct potential financial slack by using the following equation:
  
  \text{Financial slack} = \frac{\text{Income Before Taxes} + \text{Interest Charges}}{\text{Interest Charges}}


\textbf{Control variables}

We first control several firm-level factors, including firm size (SIZE), R&D expense (R&D), whether a firm has losses (LOSS), and the leverage of firm (LEVERAGE), that may explain changes in data breaches. In addition, we include variables to control for the year and industry effects.

\textbf{Results}

Tables 1 and 2 summarize our main results. Overall, the results indicate that the empirical evidence is consistent with our hypothesis.

\textbf{Table 1. Main estimation results (H1)}

\begin{tabular}{|l|c|c|c|}
\hline
 & Part 1: Internal Risk (H1a) & Part 2: External Risk (H1b) & Part 3: Universal Risk (H1c) \\
\hline
BREACH\_INT & BREACH\_EXT & BREACH \\
\hline
HR\_SLACK & 0.22*** (6.19) & HR\_SLACK & 0.21*** (5.73) & HR\_SLACK & 0.19*** (3.55) \\
SIZE & 0.21*** (5.73) & SIZE & 0.60*** (35.74) & SIZE & 0.65*** (29.82) \\
R&D & 0.67*** (35.54) & R&D & -0.77*** (-7.14) & R&D & 0.32** (2.49) \\
LEVERAGE & -1.10*** (-9.25) & LEVERAGE & -1.38*** (-9.09) & LEVERAGE & -0.60*** (-2.76) \\
LOSS & -0.66*** (-3.89) & LOSS & 0.135* (1.71) & LOSS & -0.34** (-2.71) \\
Industry Included & Industry Included & Industry Included & Industry Included \\
Year Included & Year Included & Year Included & Year Included \\
\hline
N & 265379 & 265379 & 265379 \\
Pseudo R\(^2\) & 0.212 & 0.270 & 0.270 \\
\hline
\end{tabular}

\textit{t} statistics in parentheses (* p < 0.1, ** p < 0.05, *** p < 0.01)

\textbf{Table 2. Main estimation results (H2 & H3)}

\begin{tabular}{|l|c|c|c|}
\hline
 & Hypotheses & Model1 & Model2 \\
\hline
BREACH & & & \\
HR\_SLACK & 0.13** (2.24) & 0.05 (0.60) & 0.12 (0.95) \\
FIN\_SLACK & -1.12** (-4.17) & & \\
HR\_SLACK\times FIN\_SLACK & H2 & -0.09*** (-2.70) & \\
HR\_SLACK\times DYN & H3a & 0.94** (2.20) & \\
HR\_SLACK\times COM & H3b & & -0.79** (-2.58) \\
DYN & & -2.32*** (-3.53) & \\
COM & & & 0.589 (0.78) \\
\hline
\end{tabular}
### Conclusions

Previous research on slack has generally focused on exploring the effectiveness of slack in terms of economic profit. In this study, we extend the effectiveness of slack into the scope of IT security. Specifically, we explore the input effectiveness of slack via HR slack and opportunity effectiveness of slack via financial slack. This study also contributes to the IT security research by clarifying a new organizational determinant for data breach risk. We can avoid the problem in which the same factor cannot influence the internal and external risks in the same manner by classifying these data into internal and external categories, thereby increasing the analytical accuracy in evaluating the influence of HR slack on data breach risk. Furthermore, from firm external lens, we also investigate the moderating effect of external environments on data breach risk.

### REFERENCES


---

<table>
<thead>
<tr>
<th>SIZE</th>
<th>0.65*** (29.51)</th>
<th>0.64*** (29.43)</th>
<th>0.65*** (29.67)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R&amp;D</td>
<td>0.30** (1.98)</td>
<td>0.30** (2.21)</td>
<td>0.33** (2.57)</td>
</tr>
<tr>
<td>LEVERAGE</td>
<td>-1.69*** (-5.17)</td>
<td>-0.57*** (-2.65)</td>
<td>-0.57*** (-2.67)</td>
</tr>
<tr>
<td>LOSS</td>
<td>-0.31*** (-2.45)</td>
<td>-0.32*** (-2.53)</td>
<td>-0.33*** (-2.62)</td>
</tr>
</tbody>
</table>

*Industry* Included  Included  Included

*Year* Included  Included  Included

<table>
<thead>
<tr>
<th>N</th>
<th>59070</th>
<th>59070</th>
<th>59070</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pseudo $R^2$</td>
<td>0.269</td>
<td>0.267</td>
<td>0.266</td>
</tr>
</tbody>
</table>

$t$ statistics in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$)
