
Humayun Zafar, Ph.D.  
Kennesaw State University  
hzafar@kennesaw.edu

Myung Ko, Ph.D.  
The University of Texas at San Antonio  
myung.ko@utsa.edu

Kweku-Muata Osei-Bryson, Ph.D.  
Virginia Commonwealth University  
kweku.muata@isv.vcu.edu

Abstract

We empirically investigate the impact of a chief information officer (CIO) on firm performance in the event of IT security breaches. Using Resource Based View (RBV) as a theoretical base and linking it with the role of CIOs, we determine through twin generalized linear squares (GLS) regression models that a CIO indeed does have a significant impact at the macro- and micro- levels on firm performance. In this study, Tobin’s q is used as an indicator of firm performance in the context of IT security breach for the first time in IS. Our results have implications for both the practitioner and the academic, such as positive influences of CIOs, and an alternate strategy for computing firm performance respectively. We also set the stage for future research in this area.

1. Introduction

For a CIO, the information security agenda continues to evolve. Days when a firewall and an intrusion detection system could constitute the bulk of a firm’s information security policies are long gone. The modern day CIO is business savvy, with sound risk fundamentals, and holistic technical understanding [43]. The recent volatility in the financial sector has further compounded this role. A CIO needs to understand that apart from ascertaining trade-offs between information security and cost, an organization must stay focused on its own security even at times of turmoil. At times of crisis, the robustness of an organization will be challenged from all sides, including challenges of the downturn itself, agile and aggressive competition, and hacker attacks. A survey of 600 IT executives showed that attacks on the Internet posed a growing threat to energy and communication systems that underlie modern society [38]. The Computer Security Institute (CSI) reported in their annual computer crime and security survey that each instance of financial fraud costs an average of $500,000 [44]. Annual surveys such as these suggest that a CIO has a significant impact on a firm’s performance, especially when it pertains to firms suffering from IT security breaches.

Prior researchers have equated security as being a technical, socio-philosophical [42], and/or a socio-organizational concern [18]. This has led to a situation where security is widely regarded as a field that lacks comprehensive research in information systems [35, 40]. Although important roles played by a CIO are noted in earlier studies [19, 27, 28], organizational level studies that consider financial impact of security breaches and impact of CIOs are currently lacking in IS research. This provides the primary motivation for our study.

We use Tobin’s q (hereafter q) to investigate the impact of having a CIO on firm performance in the event of information security breaches. Using resource based view (RBV) as a theoretical basis, our research explores whether breached firms that have CIOs perform better after an IT security breach than those firms that do not have a CIO.

The rest of the study is presented as follows. The next section provides an overview of Resource Based View, followed by a description of firm performance studies and an introduction of Tobin’s q. We then present our research hypotheses and method along with statistical results. We conclude with directions for future research and limitations of our study.

2. A Resource-Based View (RBV) and Firm Performance

The resource-based view of a firm posits that a firm’s resources that are perceived as valuable, rare, and difficult to imitate by competitors, and non-substitutable by other resources are the potential sources for attaining the firm’s competitive advantage and superior long-term performance [5]. The resources could be classified as tangible, intangible, and human resources [7, 25]. While tangible resources represent physical assets and financial capital, intangible resources represent brand name, patent, reputation, and product quality.
Human capital resources are skills of employees that include technical and managerial skills. According to Mata et al. [39], managerial skills include management’s ability to develop and exploit IT applications to support other business functions and they are likely to be a source of sustained competitive advantage since they are rare and complex to imitate. Accordingly, a CIO can exercise own expertise and discretion to implement strategic decisions and also improve responsiveness to external events [45]. Thus, existence of a CIO in a firm will improve organizational performance as the RBV implies.

3. Firm Performance and Tobin’s q

Economics of information security has also been researched in IS. Impacts of different types of security breaches such as data theft, virus, and denial of service (DoS) have been shown to result in serious negative effects on firms. Gordon and Loeb [23] examined how vulnerability of information affects optimal investment in security and concluded that although some investment in information security is beneficial, more security is not always worth the cost.

Emphasis has also been placed on benefits attained by organizations that share information related to information security breaches [21, 24]. Kumar et al. [36] investigated the economic consequences of security attacks relative to the Information System Security Countermeasures (ISSC) portfolios implemented by organizations. The simulation experiments illustrated the need to consider the interactions between an organization’s business environment, threat environment, and characteristics of ISSCs in order to evaluate ISSC portfolios.

There are several studies that have investigated the impact of IT security breaches on the market value of the firm using an event study methodology. Event study methodology is based on the semi-strong form of efficient market hypothesis and examines the stock market’s response to the release of information about the event [30]. Thus, it measures the impact of the event on expected future cash flows of the firms.

Some of these studies found significant negative impact on the market value of firms after the information security breach announcements [1, 10, 12, 22]. Cavusoglu et al. [12] found a significant negative impact. On average, breached firms lost 2.1 percent of their market value within two days of an announcement of a security breach. Goel and Shawky [22] concluded that security breach announcements had a negative impact of about 1 percent on market values of firms during the days surrounding the event. Campbell et al. [10] also found a significant negative impact regarding security breaches that involved unauthorized access to confidential data, whereas, not much of a reaction was noticed if the breach did not involve confidential data. Acquisti et al. [1] concluded that there was a significant negative impact on a firm’s market value on the day of the information security breach announcement. However, the authors found that this effect decreased over the days following the incident announcement. On the other hand, Hovav and D’Arcy [29] found no significant impact on the firm’s market value during the twenty five days following the announcement.

Unlike the mentioned event studies, Ko et al. [34] investigated the impact of security breaches on firm performance using financial ratios and found that the impact of security breaches was different depending on the type of security breaches and also IT intensiveness of the firm.

Many previous studies have investigated the impact of top management teams (TMT) on organizational outcomes such as involvement of TMT members, and IT implementation success [2, 47], characteristics of TMT and progressive IT use [31], and TMT compensation on performance [11]. Some of the previous studies that have focused on CIOs investigated topics such as the impact of CIOs on TMT [20, 32], and level of CIO engagement [49]. However, firm level studies that consider the role of CIO on the breached firm’s financial performance are currently lacking.

The q, defined as the ratio of the market value of firm to the replacement cost of its assets, is a commonly used tool in finance and economics as an indicator of firm performance. One of the main advantages of using q is any distortions due to tax laws and accounting conventions are minimized since it uses capital market of firm value that incorporates firm risk factors and future profitability [13] and thus, it is viewed as a better measure for the firm performance than other accounting measures such as Return on Assets (ROA) or Return on Sales (ROS) [26]. Also, it can be easily calculated based on financial and accounting information available from Compustat.

The q ratio was introduced by James Tobin as a predictor of a firm’s future investments [50]. It has since been used to explain various outcomes, such as: an alternate measure of a firm’s performance [13], a measure of brand equity [48], a measure of returns from diversification [53], a measure of resource intangibility [51], and a measure of the value of technological assets [26].
4. Research Hypotheses

In this study, we use the \( q \) as a measure of firm performance and test if presence of a CIO has a positive impact on financial performance of the breached firm, since the CIO has unique management style and expertise that can help recoup faster to negative external events such as information security breaches as based on RBV. Therefore, we predict:

H1: Breached firms that have a CIO perform better the year subsequent to a security breach compared to firms without a CIO.

We also categorized security breaches based on the confidentiality, integrity, and availability (CIA) principle. Confidentiality refers to limiting information access and disclosure to authorized users. Integrity refers to the trustworthiness of information resources. Finally, availability, not surprisingly refers to availability of information. Based on Ko et al’s [34] classification we consider data theft as an example of a breach associated with confidentiality. Web site defacement and data corruption as breaches associated with integrity, and Denial of Service as a breach associated with availability. However, previous research found that only confidentiality type of information breaches had a significant financial impact on organizations [9]. Thus, we categorized data theft as one category and all other types of security breaches as another category in this study. Based on an earlier argument with regard to the positive impact of a CIO, we posit that firms that have CIO’s will have more tools and human resources to counter different types of security breaches. Therefore, we predict:

H2: Firms with a CIO that have experienced an IT security breach involving data theft perform better the year subsequent to a security breach compared to those firms without a CIO.

5. Research Method and Data Collection

There are multiple methods for computing the \( q \) ratio \([14, 41]\). However the different approaches yield similar values for Tobin’s \( q \). In this study we use Chung and Pruitt’s \([14]\) method to calculate \( q \). Previous studies also used this method \([6, 16]\). This method approximates \( q \) as follows:

\[
\text{Tobin’s } q = \frac{(MVE + PS + DEBT)}{TA}
\]

where:

\( MVE = (\text{Closing price of share at the end of the financial year} \times \text{Number of common shares outstanding}) \)

\( PS = \text{Liquidating value of the firm’s outstanding preferred stock} \)

\( DEBT = (\text{Current liabilities} - \text{Current Assets}) + (\text{Book value of inventories}) + (\text{Long term debt}), \) and

\( TA = \text{Book value of total assets.} \)

We selected announcements of information security breaches for public firms between 2000 and 2007 using keyword search in the Lexis/Nexis Academic database. There is precedence in previous studies with regard to this approach \([3, 12]\). Afterward, for each breached organization we determined if it had a CIO from Hoover’s Handbook of American Businesses \([8]\), and Mergent Online Database. We also searched for firms which did not specifically have a CIO but had an executive with a title whose job description equivalent to that of a CIO.

The final data set included 103 breached firms (original was 127). The breached firms represented a wide array of industries based on the Standard Industrial Classification (SIC) code list. There were 38 business services, 18 banks, 11 retail goods stores, 10 telecommunication firms, 5 motion picture distribution houses, 5 air transportation companies, 4 grocery stores, 4 newspapers, 3 personal care services, 3 insurance carriers, and 2 drug stores. Out of these firms, 93 had CIOs, and 10 firms did not. The reason for the drop in breached organizations was due to the fact that Compustat did not have financial data available for them. Also, to prevent potential firm level bias we removed firms that had breaches in consecutive years. To check for potential selection bias due to the dropping of firms, we ran the analysis with and without the dropped firms, and did not see any significant differences noted.

We collected annual financial data for the year before and after the security breach for each breached organization, and computed the change in industry \( q \) (\( \Delta Indq \)) during that time period. Past studies have stressed on the importance of considering pre-incident performance \([33]\). When sample firms experience pre-event performance that is different from control firms, commonly used methods such as regression yield results that are not specified correctly \([4]\). Therefore:

\[
\Delta Indq = Indq_{t+1} - Indq_{t-1}
\]  
(1)

where \( t \) is the year of the breach.
We then computed the difference between the actual and expected $q$ for each breached organization. The actual $q$ of a breached organization is its reported financial performance a year after the breach. The expected $q$ is the measurement a year after the breach in the absence of an incident. It is computed by adding the $q$ of the breached firm a year before the breach to the change in industry $q$ from year $t - 1$ to year $t + 1$. Therefore:

$$Expq_{t+1} = Actq_{t-1} + \Delta Indq$$  

(2)

Since our intention is to measure differences in financial performance between organizations that have a CIO and those that do not, we used generalized least squares (GLS) regression with dummy variables for data analysis. Therefore:

$$y_i = \beta_0 + \beta_1 X_i + \delta_1 D_{i1} + \delta_2 D_{i2} + \epsilon_i$$  

(3)

Where,

$y_i = \text{Actual } q$

$X_i = \text{Expected } q$

$D_{i1} = 1 \text{ if firm has a CIO; 0 otherwise.}$

$D_{i2} = 1 \text{ if type of breach is data theft; 0 otherwise.}$

The key independent variable in our study is the CIO dummy variable along with the dummy variable for the type of security breach.

6. Data Analysis

Regression diagnostics were performed to check if any of the linear regression assumptions (i.e., linearity, constant variance, etc.) were in violation. For each performance ratio we checked for normality of data using the Shapiro-Wilk test. Most authors have recommended this test as the most reliable test for non-normality for small samples [17, 46]. We also checked for the problem of heteroskedasticity using the Breusch-Pagan test [9].

Also, before running the GLS regression, the data collected was checked for outliers. Residual analysis was used to identify outliers that did not appear to be consistent with the rest of the data. Although some outliers were present, analysis performed with and without the outliers revealed no difference in the results and their significance. Therefore, all observations were used for analysis purposes.

Variance inflation factor (VIF) was computed for all independent variables to test for multicollinearity. Kutner et al. [37] and Cohen et al. [15] state that multicollinearity is high when VIF is greater than 10. The VIF ranged between 3.20 and 8.92, whereby indicating that multicollinearity was not an issue with regard to estimating the regression coefficients.

Table 1 presents the results for the first model represented by equation (3).

### Table 1: Model 1 Results

<table>
<thead>
<tr>
<th>GLS (Adj. R²: 0.15)</th>
<th>Coefficients</th>
<th>Estimate</th>
<th>t-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>0.97</td>
<td>1.26</td>
<td></td>
</tr>
<tr>
<td>Expected $q$</td>
<td>-0.01</td>
<td>-3.22*</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>0.71</td>
<td>2.43*</td>
<td></td>
</tr>
<tr>
<td>Data theft</td>
<td>-0.68</td>
<td>-0.99</td>
<td></td>
</tr>
</tbody>
</table>

* p-value < 0.05

The results show a positive coefficient for CIO (i.e. 0.71). This implies that having a CIO has a positive significant impact and thus, breached firms with a CIO performed better than those firms without a CIO. Therefore, hypothesis H1 is supported.

For the type of breach dummy variable (Data theft) we were unable to determine if hypothesis H2 was supported due to the fact that we did not get a statistically significant result for it.

To gain a more granular (micro-level) insight into the impact of CIOs on firm performance, we looked at potential interaction effects as part of a second regression model. This was done to counter potential questions about the additive properties of equation (3). This resulted in a change to the original regression equation. Hence:

$$y_i = \beta_0 + \beta_1 X_i + \delta_1 D_{i1} + \delta_2 D_{i2} + \chi_1 D_{i1} X_i + \chi_2 D_{i2} X_i + \chi_3 D_{i1} D_{i2} + \epsilon_i$$  

(4)

Equation (4) shows three pairs of interactions. The key one in this case is $\chi_3 D_{i1} D_{i2}$, since it considers the type of security breach along with the presence or absence of a CIO.

Table 2 presents results for the second regression model represented by equation (4).

### Table 2: Model 2 Results

<table>
<thead>
<tr>
<th>GLS (Adj. R²: 0.68)</th>
<th>Coefficients</th>
<th>Estimate</th>
<th>t-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>0.39</td>
<td>0.18</td>
<td></td>
</tr>
<tr>
<td>Expected $q$</td>
<td>-0.01</td>
<td>-4.35*</td>
<td></td>
</tr>
<tr>
<td>Expected $q$ * CIO</td>
<td>0.02</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>Expected $q$ * Data theft</td>
<td>0.05</td>
<td>4.05*</td>
<td></td>
</tr>
<tr>
<td>CIO * Data theft</td>
<td>0.47</td>
<td>2.18*</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>0.66</td>
<td>2.23*</td>
<td></td>
</tr>
<tr>
<td>Data theft</td>
<td>0.13</td>
<td>3.91*</td>
<td></td>
</tr>
</tbody>
</table>

* p-value < 0.05
Unlike the first regression model, Table 2 results cannot be interpreted directly. For example, the coefficient of Expected q is not -0.01, but instead 0.04 (i.e., -0.01+0.05), based on the statistically significant coefficients.

As shown in Table 3, there is a positive coefficient for CIO (i.e. 0.47+0.66). This implies at a micro level that breached firms with a CIO performed better following year subsequent to breach than those firms without a CIO. Hence H1 is supported once again. Furthermore we see positive coefficients for the interaction effect of CIO and data theft (i.e. 0.47 + 0.13). This shows that firms with a CIO performed better in the year subsequent to a security breach than firms without a CIO after suffering from data theft. Thus, the second hypothesis (H2) is also supported.

7. Implications

Our results have implications for both the practitioner and the academic. For the practitioner, we have shown that apart from the previous intuitive arguments with regard to positive influences of CIOs, there is now an indication that that argument holds true based on empirical evidence. Therefore, firms may be well served by having a CIO as part of an organization’s management team. As the total number of IT security breaches will only continue to grow, and the general public will become more aware of them, importance of a CIO’s role cannot be ignored. Results of our study indicate that having a CIO has the potential to assist an organization in overcoming possible repercussions after a security breach incident.

Also, based on the results of the interaction model, and the fact that we considered performance of an organization over a period of a year, we see that benefits of having a CIO are realized in the long term.

For the academic we have provided an alternate strategy for computing firm performance in the event of an information security breach. Through the use of Tobin’s q, we found that overall organizations that suffered from a security breach benefitted from having a CIO. We also found that CIOs had a positive impact on firm performance in the event a firm suffered from a particular type of a security breach (data theft).

Our contribution is two-fold. We extend IS security research stream by linking the role of CIO to IT outcomes, especially in the case of a negative event, such as an information security breach. This in turn extends existing literature on CIOs. We also add a layer of granularity to IT security research by equating impact of CIOs on a specific type of security breach (data theft).

As part of future research we intend to consider potential correlations between other types of security breaches and the presence or absence of a CIO. We also suggest that future studies consider use of a combination of techniques to gauge firm performance. For example, accounting ratios such as Return of Assets, and Return on Sales, along with Tobin’s q can be used together. As we stated earlier, this would present a more complete picture of any phenomenon that is being investigated let alone information security.

Our study is not without its limitations. First, sample size of breached firms was small. However, the regression procedures employed in this study are consistent with the small sample properties. Hence, the impact of sample size on the results is negated.

Another potential limitation of this study is that as far as interaction effects are concerned, only two-way interactions were considered. This was done for the purpose of simplifying interpretation of results. There is no rule of thumb that dictates that a particular order of interaction effects is better than the other. Since our purpose was to identify the link between presence of CIOs in firms that had a security breach, two way interaction effects sufficed.

Vlieghe et al. [52] state that Tobin’s q of a firm may be suspect to “bubbles” or any factors other than the ones being investigated. However, Vlieghe et al. also mention that Tobin’s q will be robust if direct measures are used to measure expected performance. In our study we used the change in industry level q to compute expected q. This allowed us to use Tobin’s q as a direct reflection of industry wide information, whereby not being sensitive to individual bubbles of firms.

Finally it is important to note that this study does not ascertain causality. We have identified a potential correlation between presence of a CIO and an IT security breach. We recommend that future studies aim to identify any causal relations based on...
the scientific method as established in literature, e.g. Shadish et al. [45].

9. References


