JOURNAL OF INFORMATION SYSTEMS
Vol. 27, No. 1
Spring 2013
pp. 219–236

American Accounting Association
DOI: 10.2308/isys-50339

The Association between Top Management Involvement and Compensation and Information Security Breaches

Juhee Kwon
Dartmouth College

Jackie Rees Ulmer
Purdue University

Tawei Wang
University of Hawaii at Manoa

ABSTRACT: This paper examines how an information technology (IT) executive's position in a top management team and how his/her compensation are associated with the likelihood of information security breaches. Using a sample drawn from multiple sources in the period from 2003 to 2008, we show that an IT executive's involvement in the top management team is negatively related to the possibility of information security breaches. We also find that the amount of behavior-based (i.e., salary) compensation and the pay differences of outcome-based (i.e., bonuses, stock awards, and stock options) compensation between IT and non-IT executives are negatively associated with the likelihood of information security breaches. Our findings shed light on how an IT executive's status in the top management team and the composition of his/her compensation can be related to a firm's IT governance mechanisms.

Keywords: information security risk management; IT governance; IT executives; information security breach.

I. INTRODUCTION

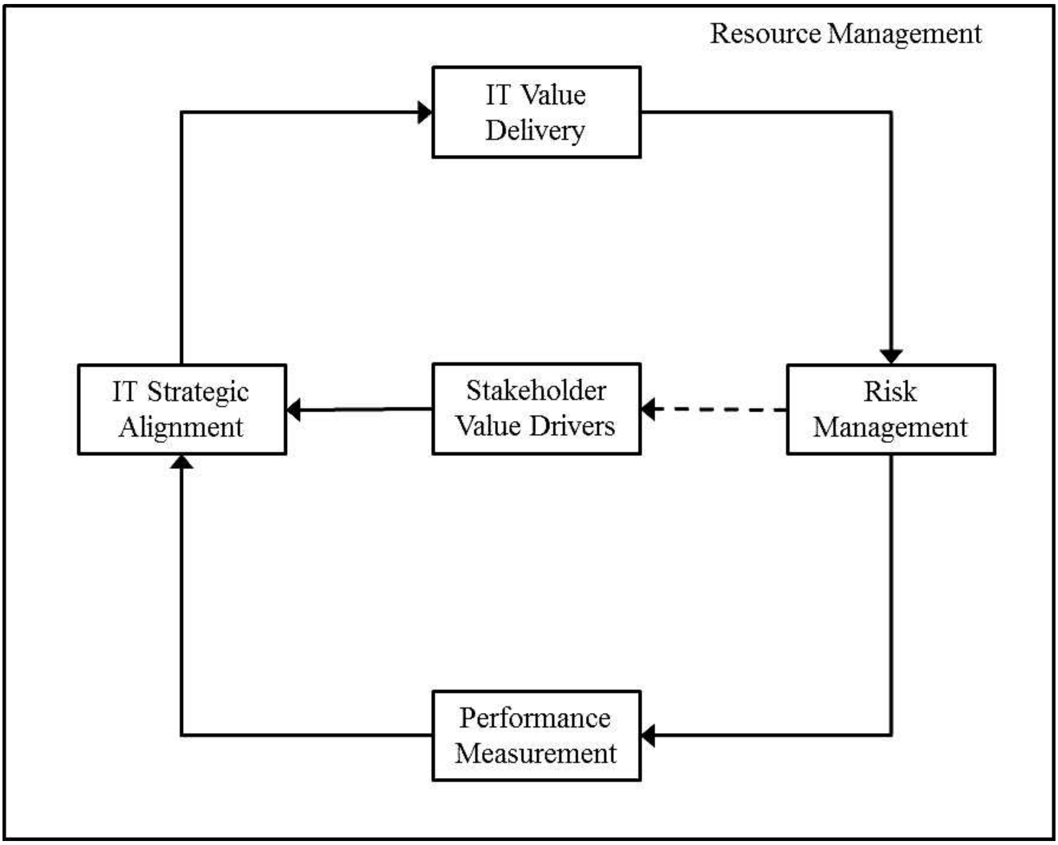
Information security risks have grown in numbers and complexity in the last decade. In response to this trend, there has been enhanced regulatory pressure on information security, such as the passage of the state data breach notification laws in the U.S. (Wallace et al. 2011). However, it is not clear that this increased pressure has changed firms' information security management activities. For example, a recent PricewaterhouseCoopers survey of 834 directors shows that only 19 percent of the

The authors thank the review team for their comments and suggestions. The authors also thank the participants of the Workshop on e-Business 2009 (WeB 2009). The authors are grateful for the financial support from Dartmouth College, Purdue University, University of Hawaii at Manoa, and National Taiwan University.

Editor's note: Accepted by Roger S. Debreceny.

Published Online: October 2012

FIGURE 1
IT Governance Framework



Source: ITGI (2005).

respondents have an effective monitoring plan to reduce information security risks (PwC 2011). Given the concern over effective monitoring plans and the potential impact of information security breaches on a firm's operations (CSI 2011), information security has been emphasized as an important element in overall information technology (IT) governance frameworks, such as ISO 27002 and COBIT 5.

Figure 1 presents an IT governance framework where IT governance is a continuous lifecycle (ITGI 2005). There are five primary elements in this framework: strategic alignment, performance measurement, resource management, IT value delivery, and risk management. Although all of these elements are driven by the stakeholder value, the first three elements are the drivers while the last two are the outcomes of IT governance (see Wilkin and Chenhall [2010] for detailed discussion). The cycle usually starts with the strategy alignment. Then implementation delivers the value set by the strategy and properly manages the risks. The strategy needs to be monitored and the results need to be measured, reported, and acted upon (ITGI 2005; Wilkin and Chenhall 2010). Note that without successful risk management, IT values cannot be delivered to shareholders and customers (Ettredge and Richardson 2003; Wilkin and Chenhall 2010).

As information security management involves different functional areas and operational processes, it can significantly affect the accomplishment of business objectives and the value delivered to stakeholders. Given the complex nature of information security management, the IT governance frameworks provide a comprehensive guidance that aims to assist firms in mitigating IT risks and delivering IT value. In particular, the framework suggests that a firm needs skilled and motivated people in order to have desirable information security behaviors related to information security maturity and the security culture of the firm. The importance of top management support in cultivating such behaviors has also been emphasized (ISACA 2012b).

The above discussion suggests that the executives play a crucial role not only in IT governance but also in information security management. Given the importance of the role played by executives on the effectiveness of information security management, this paper attempts to answer the following two research questions. First, is the involvement of IT executive(s) in the top management team associated with the effectiveness of information security management? Second, how is the compensation scheme related to the IT executives' role in information security management? As IT executives' activities and the effectiveness of information security management are not directly observable, we consider (1) whether there exists an IT executive position in the top management team as our involvement measure, and (2) the occurrence of reported information security breaches as our measure for the effectiveness of information security management as used in prior risk management literature (e.g., Wang and Hsu 2010a, 2010b, 2012).

By using a sample collected from 2003 to 2008, we show that the involvement of an IT executive in a top management team is negatively associated with the possibility of reported security breaches. Furthermore, we find that the amount of behavior-based (i.e., salary) compensation as well as the pay differences of outcome-based (i.e., bonuses, stock awards, and stock options) compensation between IT and non-IT executives in a firm are also negatively related to the likelihood of information security breaches. Although studies have paid attention to information security-related issues (e.g., Campbell et al. 2003; Ettredge and Richardson 2003), there are a limited number of empirical studies that consider the relation between top management team composition and information security management (e.g., Wang and Hsu 2010a).[1] This paper attempts to fill in this gap from the IT governance perspective. In addition, our paper sheds light on how an IT executive's status in a top management team can be associated with information security governance.

The remainder of the paper is organized as follows. In the next section, we discuss background and relevant literature, and we develop our hypotheses. In Section III, we present our research methodology and empirical models. Empirical results are given in Section IV. In Section V, we conclude with discussion and implications.

II. BACKGROUND, LITERATURE REVIEW, AND HYPOTHESIS DEVELOPMENT

The following section provides additional background on IT governance, specifically more information on COBIT 5 as an example of a well-known IT governance framework. We also discuss the positioning of information security within the IT governance literature. The hypotheses are then developed within the context of the relevant literature.

COBIT 5 defines "governance" as the role of the board where a firm evaluates the opportunities, and directs what has to be done and monitors performance. Although the board is responsible for governance, the top management team is critical in management (Wilkin and Chenhall 2010). That is, top management support is strongly related to the process maturity for IT governance since top

[1] Our focus is on information security, which is very different from internal control weaknesses (e.g., Li et al. 2007). In particular, the internal control weaknesses disclosed as required by the Sarbanes-Oxley Act are about whether such weaknesses would affect financial reporting quality. Differently, information security breaches can possibly affect a firm's operations of different functions. In addition, material weaknesses depend more on internal factors, while information security breaches relate to both internal and external factors like technologies or hackers' preferences and are thus more unpredictable.

management influences how communication, enforcement, norms, incentives, and rewards can be used to cultivate appropriate behaviors (ISACA 2012b). The political climate of the firm can also influence the tone for any norm, which frequently faces employee resistance to restricting or monitoring behavior. Top management teams imperatively play an important role in creating IT guiding principles, monitoring the business impact of IT, and evaluating benefits delivered by IT (Posthumus and von Solms 2005). COBIT 5 further emphasizes that IT governance can be achieved only if the top management team recognizes the importance of the information risk management aspect of IT governance (ISACA 2012a). The top management support for IT governance among a firm's strategic decisions can be mirrored by an IT executive's status in a top management team. One way to achieve this is to have formal membership of an IT executive in the top management team (Preston et al. 2008; Strassmann 1994). This membership can lead to a more thorough understanding of the business and technical environment, well-prioritized IT, and IT involvement in enterprise strategy development (Johnson and Lederer 2010; Luftman 2000; Chen et al. 2010; Smaltz et al. 2004). As discussed in the Introduction, information security risks may affect different elements of the IT governance framework, and the involvement of IT executives in the top management team can potentially result in managing information security risks more effectively. However, as mentioned earlier, the effectiveness of information security risks is not directly observable. We consider information security breaches as a measure of information security performance or the effectiveness of information security management, as in prior literature (e.g., Campbell et al. 2003; Kannan et al. 2007; Wang and Hsu 2010a, 2010b; Wang et al. 2012). Thus, we hypothesize:

H1: The association between an IT executive's involvement in a top management team and the likelihood of reported information security breaches is negative.

While the formal membership of an IT executive in a top management team is one thing, his/her political influence over IT governance on the corporate agenda is another. That is, simple presence in the team cannot itself assure the proper prioritization for IT governance in a firm's strategic decisions. However, IT executives with adequate political influence could strongly impact prioritization (Luftman and Kempaiah 2008; ITGI 2005). In order to measure the structure of political influence, prior literature demonstrates that the compensation structure is a good indication of how the top management team prioritizes its functional areas in strategic development and how much the top management team values the contributions from each area (Eisenhardt 1989; Yayla and Hu 2008). Compensation is also related to the endowment of political influence. We thus consider IT executives' compensation as a function of both authority for strategic decision making and motivation for achieving good IT governance. Hence, as information security management is a critical part of IT governance, we argue that the level of IT executive compensation can make a difference in information security performance.

H2a: An IT executive's total compensation is negatively associated with the likelihood of reported information security breaches.

Moreover, the effect of the compensation structure becomes more complicated with executives' risk appetites and risk-taking behaviors. Agency theory researchers have tried to identify which contract type of compensation is most effective given a certain level of task uncertainty and risk aversion (Santaló and Kock 2009). Considering executives as self-interested individuals, behavior-based (i.e., salary) and outcome-based (i.e., bonuses, stock awards, and stock options) contracts may have different effects on information security performance given risk-taking behaviors of executives (Oliver and Anderson 1994).

Information security events are unpredictable because such events depend on numerous evolving variables such as technological changes, economic climate, government regulations, and attackers' evolving strategies (Anderson 2001; Dhillon and Backhouse 2001). Accordingly, IT executives encounter organizational and environmental uncertainties with high potential for such risks. Thus, assuming IT executives are risk-averse, we argue that a behavior-based contract is preferred among IT executives facing such uncertainties (Eisenhardt 1989; Oliver and Anderson 1994). Formally, we hypothesize:

H2b: The magnitude of the association between an IT executive's behavior-based compensation and the likelihood of reported information security breaches is larger than that of outcome-based compensation.

Linking executives to their compensation structure requires taking into account how the strategic positions of their areas are prioritized and how they fit within the firm's strategies (Kearns and Lederer 2003). The literature demonstrates that executives with higher levels of influence have been shown to have higher compensation-performance sensitivity (Aggarwal and Samwick 1999; Hall and Liedtka 2005). Considering strong IT governance as the ultimate objective of IT executives, any difference in compensation structure between IT and non-IT executives is viewed as a proxy for the prioritization of IT governance as well as compensation-performance sensitivity. That is, the compensation structure can represent micro-level opportunity structures of functional positions as well as strategic resource allocations (Holthausen et al. 1995).

For example, Carpenter and Wade (2002) argue that the compensation structure of a top management team makes a firm's resource allocation visible among functional areas. This strategic resource allocation can be reflected by the compensation distance (i.e., differences) between functional heads. Focusing on IT governance, we examine the compensation distance between IT and non-IT executives. If the compensation distance is closer between IT and non-IT executives, it implies that the strategic resource allocation is more balanced and that IT governance has proper priority among business functional areas. Again, as information security management is an important part of IT governance, the strategic resource allocation would affect IT governance as well as information security management.

H3a: The association between the total compensation distance between IT and non-IT executives is negatively associated with the likelihood of reported information security breaches.

Similar to H2b, outcome-based and behavior-based compensation play different roles in motivating IT executives. Thus, we separate behavior-based and outcome-based compensation distances from total compensation distance. Generally, outcome-based compensation, including bonuses, stock awards, and stock options, generally depends on a firm's goal achievement such as revenues. Thus, when comparing to other executives of the same top management team that face the same equity values and market structure, the differences of outcome-based compensation more clearly indicate the prioritized levels between IT units and other strategic business areas (Galbraith and Merrill 1991). Therefore, our hypothesis is:

H3b: The magnitude of the association between outcome-based compensation distance between IT and non-IT executives and the likelihood of reported information security breaches is larger than that of behavior-based compensation distance.

III. RESEARCH METHODOLOGY

Data

We collected information security breaches from DataLossDB, LexisNexis, CNET, and ZDNet in the period from 2003 to 2008. DataLossDB (http://datalossdb.org) provides a list of reported

TABLE 1

Composition of Dataset 1 and Dataset 2

	Dataset 1	Dataset 2
Total number of firms	2,256	557
Number of firms that have an IT executive in the top management team	557	557
Number of firms that do not have an IT executive in the top management team	1,699	—
Number of firms that have reported security breaches	242	61

information security events. The list is composed of breach notification letters from various jurisdictions in the U.S. and reported breaches from news feeds, blogs, and other websites, and is updated on a daily basis. To make sure we did not miss any major information security events, we also searched for the following keywords on LexisNexis, CNET, and ZDNet: "information breaches," "security breaches," "identify theft," "hacking," "site attack," "virus," "data theft," or "privacy breaches." These terms are similar to those used in prior studies (e.g., Campbell et al. 2003; Wang and Hsu 2010b; Wang et al. 2012; Wang et al. 2012). From these processes, we identified 577 information security breaches in which 268 are events from 242 publicly traded firms. Note that 26 ($268 - 242 = 26$) firms experienced more than one breach in the time period 2003–2008. These 242 firms were further matched to the ExecuComp database for executive information and the corresponding compensation structure. However, to address our research questions, we also needed a set of firms without reported information security breaches but with executive information. To do so, we gathered the rest of the firms from the ExecuComp database in the period from 2003 to 2008. Accordingly, all the firms in this final sample had executive information. This final sample consisted of firms with and without reported information security breaches.

The resulting sample had 2,256 publicly traded firms in the period between 2003 and 2008 (labeled as Dataset 1 hereafter). Among these firms, 557 had an IT executive in the top management team. The set of firms having an IT executive in the top management team was referred to as Dataset 2 hereafter, which is a subset of Dataset 1. The compositions of both Dataset 1 and Dataset 2 are given in Table 1. To verify that our sample is representative, we compared the following performance and size measures against the Compustat database universe in the same period (i.e., 2003 to 2008): return on assets (ROA), net income, sales revenues, and market value. The results are given in Table 2. Table 2 demonstrates that our sample is not significantly different from the population in the Compustat database.

Empirical Model

We use Model (1) to test H1, which argues that the involvement of an IT executive in a top management team is negatively associated with the likelihood of reported security breaches. That is, Model (1) estimates the probability of the occurrence of reported security breaches by using logistic regression with the full sample (i.e., Dataset 1). Logistic regressions have been widely used in different contexts when the dependent variable is binary, such as voting, morbidity or mortality, participation data, operational risks, and information security risks (Kohli and Devaraj 2003; Vafeas 2005; Archambeault et al. 2008; Wang and Hsu 2010a, 2012). Since we are interested in the possibility of the occurrence of reported information security breaches (a binary variable), we also consider logistic regression. Note that unless otherwise indicated, the dependent variables in the following models are measured for firm i at time t, while each independent variable is evaluated at time $t-1$. We introduce a lag because it is possible that the involvement of an IT executive at time

TABLE 2

Comparing Our Sample with the Compustat Universe

	Dataset 1 versus Compustat		Dataset 2 versus Compustat	
Measure	**t-value**	**p-value**	**t-value**	**p-value**
ROA	1.59	0.11	0.98	0.32
Net Income	0.52	0.60	0.81	0.41
Sales	−0.53	0.59	−0.01	0.31
Market Value	1.26	0.20	1.05	0.29

t−1 may change the deployment of information security resources at time *t*. In addition, we control for certain firm characteristics at time *t*−1 as a general background condition before the occurrence of information security breaches.

Model (1)

$$log\Big(P(Breach_i \geq 1)\Big) = \alpha_0 + \alpha_1 ITEXE_i + \alpha_2 ITINT_i + \alpha_3 ROA_i + \alpha_4 FTE_i + \alpha_5 EPS_i + \alpha_6 DPS_i + \alpha_7 BM_i + \alpha_8 Turnover_i + \varepsilon_{1i}, \tag{1}$$

where *Breach* is a dummy variable indicating whether a firm has media reports of information security breaches (e.g., Wang and Hsu 2010a, 2010b). *Breach* equals 1 if a firm has at least one reported security breach at time *t*, 0 otherwise (see Appendix A for variable definitions). *ITEXE* is the involvement of IT executive(s). *ITEXE* equals 1 if a firm has at least an IT executive in its top management team, 0 otherwise. Titles of IT executives are, for example, Chief Information Officer (CIO), Chief Security Officer (CSO), VP—Information & Technology, among others. We also searched for other possible titles, such as Chief Privacy Officer (CPO), but did not find any in the dataset.

We include a number of control variables that are fairly standard in information security research. *ITINT* is IT intensity, which is the ratio of annual IT capital to the number of full-time employees at the four-digit SIC code level, deflated by the average ratio of all industries (Dumagan and Gill 2002). It is possible that firms in the high IT intensity industry are more likely to face information security issues. *ROA* is return on assets, which equals the net income before extraordinary items and discontinued operations divided by total assets, then multiplied by 100. *EPS* is earnings per share, which equals net income (minus preferred dividend, if any) divided by the weighted outstanding common shares. *DPS* stands for dividends per share, which is the total dividend paid over year *t*. These three variables (*ROA*, *EPS*, and *DPS*) capture whether a firm has more resources or capital to invest in security management if needed. *FTE* is the logarithm of the total number of full-time employees, which is a proxy for the size of the firm. Larger firms may become a target of attacks, but at the same time may have more resources and better mechanisms for preventing security events from happening. The variable is log-transformed to deal with the skewness of the data as suggested in prior literature (e.g., Pavlou et al. 2007). As indicated below, we also use log-transformation on our compensation variables and financial information such as sales. The number of board meetings (*BM*) refers to the level of monitoring functions in a firm (Vafeas 1999). The monitoring function may be able to reduce the possibility of information security events. *Turnover* is the level of IT executive turnover in a certain year. This variable captures the discontinuation of IT strategy, which might be associated with worse governance mechanisms.

To test H2a, H2b, H3a, and H3b, we only focus on the firms with an IT executive in the top management team (i.e., Dataset 2) for the analysis. That is, we would like to investigate the association between IT executive compensation and the possibility of reported information security breaches. However, executive compensation can be endogenous. Accordingly, we employ a multi-stage least squares method with instrumental variables, which obtains consistent parameter estimates (Greene 2003), as in Model (2) (Equations (2) and (2-1)) and Model (3) (Equations (3), (3-1), and (3-2)).

Model (2)

$$\begin{aligned} Breach_i = {} & \gamma_0 + \gamma_1 P\_TotComp_i + \gamma_2 Distance_i + \gamma_3 ITINT_i + \gamma_4 ROA_i + \gamma_5 FTE_i + \gamma_6 EPS_i \\ & + \gamma_7 DPS_i + \gamma_8 BM_i + \gamma_9 Turnover_i + \varepsilon_{2i}. \end{aligned} \tag{2}$$

$$TotComp_i = \theta_0 + \theta_1 Age_i + \theta_2 Firmvol_i + \theta_3 Tenure_i + \theta_4 Breach_i + \theta_5 Sales_i + \varepsilon_{21i}. \tag{2-1}$$

Model (3)

$$\begin{aligned} Breach_i = {} & \gamma_0 + \gamma_1 P\_BeComp_i + \gamma_2 P\_OutComp_i + \gamma_3 BeDistance_i + \gamma_4 OutDistance_i \\ & + \gamma_5 ITINT_i + \gamma_6 ROA_i + \gamma_7 FTE_i + \gamma_8 EPS_i + \gamma_9 DPS_i + \gamma_{10} BM_i + \gamma_{11} Turnover_i \\ & + \varepsilon_{3i}. \end{aligned} \tag{3}$$

$$BeComp_i = \theta_0 + \theta_1 Age_i + \theta_2 Firmvol_i + \theta_3 Tenure_i + \theta_4 Breach_{ip} + \theta_5 Sales_i + \varepsilon_{31i}. \tag{3-1}$$

$$OutComp_i = \beta_0 + \beta_1 Age_i + \beta_2 Firmvol_i + \beta_3 Tenure_{ip} + \beta_4 Breach_i + \beta_5 Sales_i + \varepsilon_{32i}. \tag{3-2}$$

Equations (2) and (3) are the main models to investigate the association between compensation and the occurrence of reported security breaches. Equations (2-1), (3-1), and (3-2) consider the endogenous variables: $TotComp_i$, $BeComp_i$, and $OutComp_i$. *TotComp* is the total amount of the compensation package, including both behavior-based (i.e., salary) and outcome-based (i.e., bonuses, stock awards, and stock options) compensation. *BeComp* is behavior-based compensation, which is the salary amount in the compensation package, while *OutComp* is outcome based, which is the total amount of bonuses, stock awards, and stock options. As mentioned earlier, all the above compensation variables are log-transformed (Hallock 1997). $P\_TotComp_i$, P_BeComp_i, and $P\_OutComp_i$ are the predicted values from Equations (2-1), (3-1), and (3-2) of the total amount of the compensation package, behavior-based (i.e., salary) compensation, and outcome-based (i.e., bonuses, stock awards, and stock options) compensation, respectively. $Distance_i$, $BeDistance_i$, and $OutDistance_i$ represent total, behavior-based, and outcome-based compensation differences between the compensation of the IT executive and the average of non-IT executives within a firm, respectively. The instrumental variables are the age of the IT executive (*Age*), the tenure of the IT executive (*Tenure*), and firm volatility (*Firmvol*). Gibbons and Murphy (1992) suggest that *Age* is one of the major factors in executive compensation. Younger executives are willing to take more risky actions because of career ambition for the future. They also claim that executives' performance would decrease as they age, because career ambitions provide fewer incentives as the executive moves closer to retirement. *Tenure* was computed from the recorded date of hiring (Bloom 1999) to the end of year *t*. Since an IT executive's tenure may be correlated with knowledge of firm politics, culture, and IT governance, the longer the tenure of the executive, the more entrenched he/she is likely to become, and the more power to pursue his/her own interests rather than those of the firm's stockholders (Pfeffer and Langton 1993; Fiss 2006). In addition, executives' influence over boards is expected to increase with their tenure. The last instrument is

TABLE 3

The Descriptive Statistics and Correlations of the Variables in Dataset 1

		Mean	Std.	Min.	Max.	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1)	*ITEXE*	0.24	0.42	0.00	1.00	1.00							
(2)	*ITINT*	2.06	3.01	0.06	22.98	**−0.05**	1.00						
(3)	*ROA*	5.23	3.88	−1.99	14.98	**0.04**	**−0.10**	1.00					
(4)	*Sales*	6.15	0.77	3.34	8.57	0.02	**0.12**	**0.04**	1.00				
(5)	*FTE*	3.65	0.74	0.84	6.32	**0.05**	**−0.02**	**0.08**	**0.72**	1.00			
(6)	*EPS*	1.65	1.37	−2.90	7.00	−0.06	**0.08**	**0.30**	**0.42**	**0.29**	1.00		
(7)	*DPS*	1.15	1.55	0.00	7.92	**−0.12**	**0.19**	**−0.23**	**0.16**	**0.03**	**0.15**	1.00	
(8)	*BM*	7.69	3.21	1.00	25.00	**0.04**	**0.12**	**−0.15**	**0.07**	0.02	**−0.04**	**0.06**	1.00
(9)	*Firmvol*	0.43	0.27	0.11	3.89	**0.11**	**−0.07**	**0.01**	**−0.26**	**−0.20**	**−0.33**	**−0.39**	**0.05**

Values in bold represent significance at the 5 percent level.

Firmvol, which is the return volatility measured as the standard deviation of stock price change over the past 60 months. Based on individuals' risk propensity, their preferences on compensation contract types may vary with market volatility. That is, since higher return volatility affects the fluctuation of the value of outcome-based compensation, executives need to be compensated with more outcome-based compensation (Demsetz and Lehn 1985). We further include *Breach* and *Sales* of a firm in Equations (2-1), (3-1), and (3-2). We include *Breach* because the occurrence of reported information security breaches may change the compensation level of an IT executive. Note that the *Breach* is measured at *t*–1. *Sales* is the logarithm of total sales revenues, which reflects not only the size but also the gross performance of a firm.

Descriptive Statistics

The descriptive statistics and the correlations of the variables in Dataset 1 are given in Table 3. Table 3 shows that about 25 percent of the firms have an IT executive in the top management team. Return on assets (*ROA*), on average, is about five times and *EPS* is $1.65. In terms of the correlations, Tables 3 and 4 show low values for correlation except for *Sales* and the number of full-time employees (*FTE*). However, this is not a concern for this study because sales and the number of full-time employees appear in different equations. Table 4 presents the descriptive statistics and the correlations of the variables in Dataset 2. Table 4 shows that, on average, the logarithm of salary (*BeComp*) and the logarithm of the summation of bonuses, stock awards, and stock options (*OutComp*) are about 12.5 and 12.6. Return on assets (*ROA*), on average, is about six times and *EPS* is $1.59. Again, Table 4 demonstrates that the number of full-time employees (*FTE*) is highly correlated with *Sales* (0.81, $p < 0.05$). Nevertheless, as they are not in the same equation, this should not affect our results.

IV. EMPIRICAL RESULTS

Our results for H1 are given in Table 5. Table 5 shows that the involvement of an IT executive is significantly and negatively associated with the probabilities of reported security breaches (the coefficient of *ITEXE* is –0.217, $p < 0.05$). That is, as given by the odds ratio, the involvement of an IT executive decreases the probability of information security breach reports by about 35 percent (1 – 0.648). Table 5 also suggests that firm performance (return on assets, *ROA*, and earnings per share, *EPS*) and size (number of full-time employees, *FTE*) are positively associated with the

TABLE 4

The Descriptive Statistics and Correlations of the Variables in Dataset 2

		Mean	Std.	Min.	Max.	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
(1)	*BeComp*	12.53	1.15	0.00	13.82	1.00											
(2)	*OutComp*	12.60	4.45	−25.9	16.81	**0.30**	1.00										
(3)	*BeDistance*	0.06	0.08	−0.16	0.36	**0.10**	−0.01	1.00									
(4)	*OutDistance*	0.52	0.92	−3.76	4.98	−0.01	**−0.19**	0.03	1.00								
(5)	*ITINT*	1.79	3.01	0.06	22.98	**−0.11**	0.06	−0.05	−0.05	1.00							
(6)	*ROA*	5.56	3.95	−1.97	14.97	−0.05	−0.01	**−0.20**	−0.05	−0.03	1.00						
(7)	*Sales*	6.17	0.74	3.34	8.08	**0.22**	**0.28**	**0.19**	**−0.25**	−0.05	−0.07	1.00					
(8)	*FTE*	3.72	0.73	1.54	5.56	**0.51**	**0.21**	0.08	**−0.17**	**−0.11**	−0.01	**0.81**	1.00				
(9)	*EPS*	1.59	1.32	−2.62	6.98	**0.16**	**0.15**	**−0.25**	**−0.15**	**0.16**	**0.35**	**0.47**	**0.43**	1.00			
(10)	*DPS*	0.83	1.28	0.00	7.89	**0.11**	0.01	0.02	−0.08	0.07	**−0.23**	**0.35**	**0.33**	**0.16**	1.00		
(11)	*BM*	7.90	3.31	1.00	25.00	**−0.23**	0.06	**−1.14**	−0.09	−0.01	**0.23**	−0.04	**−0.19**	0.08	**−0.16**	1.00	
(12)	*Firmvol*	0.49	0.28	0.12	3.21	**−0.18**	−0.05	**0.23**	**0.13**	0.02	0.03	**−0.38**	**−0.36**	**−0.33**	**−0.25**	**0.15**	1.00
(13)	*Turnover*	0.32	0.57	0.00	2.00	**0.18**	−0.02	**0.16**	−0.01	0.08	−0.07	**0.15**	**0.15**	**0.09**	**0.17**	−0.02	−0.01

Values in bold represent significance at the 5 percent level.

TABLE 5

Logistic Regression with IT Executive Involvement (Dataset 1; n = 2,256)

	Model (1) Dependent Variable: *Breach*		
Independent Variables	**Estimated Coefficients**	**Odd Ratio**	**Hypotheses**
ITEXE	−0.217** (0.110)	0.648	H1: Supported
ITINT	0.003 (0.020)	1.003	
ROA	0.069*** (0.016)	1.071	
FTE	0.702*** (0.152)	2.714	
EPS	0.125* (0.068)	1.133	
DPS	−0.026 (0.038)	0.975	
BM	−0.004 (0.032)	0.996	
Firmvol	−0.316 (0.954)	0.729	
Pseudo R^2	0.10		
Chi-square	24.62		

*, **, *** Significant at 10 percent, 5 percent, and 1 percent, respectively.
Standard errors are in parentheses, and p-values are based on the two-tailed test.

likelihood of information security breaches. In summary, our findings show that, consistent with H1, the involvement of an IT executive in the top management team is negatively associated with the information security breaches.

To test the rest of the hypotheses, we first perform the Hausman test to determine whether a multi-stage model is more appropriate as given in Table 6. Table 6 indicates that two-stage least squares (2SLS) and three-stage least squares (3SLS) are preferred over ordinary least squares (OLS) at the 1 percent level of significance. That is, the null hypothesis of no measurement error is rejected. Next, it seems that the test is indifferent between 2SLS and 3SLS. However, while surely 2SLS is not preferred over 3SLS, the p-value of 3SLS is smaller than that of 2SLS. Furthermore, 3SLS is a combined model of 2SLS and seemingly unrelated regression (SUR) (Greene 2003). Therefore, we conservatively choose 3SLS as our main method.

Our findings from the multi-stage models are given in Tables 7 and 8. Note that since we only consider Dataset 2 for the rest of the analyses, the results can only be applied to the firms with IT executives. Table 7 shows the results for Equations (2-1), (3-1), and (3-2). We find that market volatility (*Firmvol*) significantly influences total compensation (0.621, $p < 0.01$) and outcome-based compensation (1.139, $p < 0.01$), but not behavior-based compensation. Interestingly, *breach* at *t*−1 is significantly and negatively associated with total compensation (−0.939, $p < 0.01$) and behavior-based compensation (−2.237, $p < 0.01$) at time *t*, but it has no significant effect on outcome-based compensation (−0.804, n.s.). It seems that the occurrence of a reported breach is negatively associated with the IT executive’s salary, at least in our dataset.

TABLE 6

Hausman Specification Test

Efficient Under Ho	Consistent Under Ha	Chi-square Statistic	Pr > Chi-square
OLS	2SLS	40.85	0.0010
OLS	3SLS	73.64	< 0.0001
3SLS	2SLS	13.89	0.8745

Table 8 shows the 3SLS results. First, the results from Equation (2) demonstrate that IT executives' total compensation is negatively related to the likelihood of reported information breaches (–0.630, $p < 0.01$). This result supports our H2a that compensation can motivate individuals as well as assign political influence to a firm's strategic decisions, which improves the firm's IT governance function (Carpenter and Sanders 2002; Yayla and Hu 2008). In addition, the results from Equation (2) also suggest that the larger the total compensation difference between IT and non-IT executives (*Distance*), the lower the possibility of reported information security breaches (–0.257, $p < 0.05$), which is consistent with H3a.

The results for Equation (3) in Table 8 show that behavior-based compensation is also significantly and negatively associated with the possibility of information security breach reports (−1.068, $p < 0.01$), which supports H2b. On the other hand, we do not observe any significant relation between outcome-based compensation and the possibility of reported security breaches. The above finding suggests that the unpredictability of information security risks may change the effect of behavior-based compensation on the effectiveness of information security management. In addition, the outcome-based compensation distance (–0.317, $p < 0.10$) is negatively associated with the possibility of information security breaches while such association is insignificant for behavior-based compensation distance (–0.197, n.s.), consistent with H3b. Our results confirm our

TABLE 7

Compensation with Instrument Variables (Dataset 2; n = 557)

Independent Variables	Equation (2-1) Dependent Variable: *Total Compensation*	Equation (3-1) Dependent Variable: *Behavior-Based Compensation*	Equation (3-2) Dependent Variable: *Outcome-Based Compensation*
Age	0.017**	0.009	0.005
	(0.006)	(0.006)	(0.010)
Firmvol	0.621***	0.234	1.139***
	(0.179)	(0.188)	(0.306)
Tenure	0.003	−0.002	−0.018
	(0.007)	(0.007)	(0.012)
Breach	−0.939***	−2.237***	−0.804
	(0.333)	(0.348)	(0.561)
Sales	0.714***	0.354**	1.004***
	(0.196)	(0.182)	(0.294)
R^2	0.27	0.19	0.23

*, **, *** Significant at 10 percent, 5 percent, and 1 percent, respectively.
Standard errors are in parentheses, and p-values are based on the two-tailed test. *Breach* is measured at *t*–1.

TABLE 8

3SLS Regression (Dataset 2; n = 557)

	Equation (2)	Equation (3)	
	Dependent Variable: *Breach*		**Hypotheses**
Independent Variables			
P_TotComp	−0.630*** (0.198)		H2a: Supported
P_BeComp		−1.068*** (0.218)	H2b: Supported
P_OutComp		0.110 (0.096)	H2b: Supported
Distance	−0.257** (0.115)		H3a: Supported
BeDistance		−0.197 (0.164)	H3b: Supported
OutDistance		−0.317* (0.170)	H3b: Supported
Control Variables			
ITINT	−0.847*** (0.259)	−0.141 (0.132)	
ROA	−0.022** (0.011)	−0.023** (0.010)	
FTE	−0.500** (0.205)	0.204 (0.289)	
EPS	0.083* (0.044)	0.163 (0.137)	
DPS	−0.572*** (0.112)	−0.563*** (0.094)	
BM	0.018 (0.045)	−0.023 (0.058)	
Turnover	2.695 (1.667)	1.378 (0.992)	
R^2	0.35	0.28	

*, **, *** Significant at 10 percent, 5 percent, and 1 percent, respectively.
Standard errors are in parentheses, and p-values are based on the two-tailed test.

expectation that compensation differences between IT and non-IT executives could show how a firm prioritizes its resources and in turn affects the effectiveness of information security management.

V. DISCUSSION AND IMPLICATIONS

This paper empirically examines the association between an IT executive's status in a top management team and the likelihood of the occurrence of information security breach reports. Our results find that the involvement of an IT executive in the top management team is negatively associated with the likelihood of information security breaches. This finding suggests that the support of the top management may influence the setting of security guidelines and principles. It also affects security management behaviors through facilitated communications and across functions. In addition, behavior-based compensation and the pay differences of the outcome-based compensation are also negatively related to the possibility of reported security breaches. That is, as information security risk management tasks tend to be highly uncertain, behavior-based compensation plays a more important role in motivating IT executives compared to outcome-based compensation. When the compensation of IT executives is more properly aligned with the nature of the task, the effectiveness of information security management is also expected to improve.

Our paper contributes to the literature in the following ways. First, although prior research has paid attention to information security management, only a limited number of studies (e.g., Wang and Hsu 2010b) focus on the relation between the top management team and the effectiveness of information security management. This paper fills this gap by addressing how the involvement of an IT executive and his/her compensation are associated with the possibility of reported information security breaches. Second, a quote from a recent *Wall Street Journal* article stated that, "The newly created position of chief information security officer will keep a dynamic focus on the latest security threats and advanced defenses against those threats to uphold our unwavering commitment to protect our customers' data" (Bussey 2011). Echoing risk management and IT governance frameworks and the media article above, our studies suggest that it is important to formally bring this issue to the c-suite level. By doing so, a firm is able to view and incorporate information security management into its overall business activities and align IT governance with a firm's ultimate objectives. More importantly, a position in the c-suite needs to be accompanied by an appropriately designed incentive scheme to motivate the executive in line with organizational goals and to assign proper political influence.

This study also has managerial implications. To deal with the rapidly changing and increasingly complicated information security risks, a firm needs to be equipped with the capability of managing such risks effectively. The capability can be improved by setting or redesigning an IT executive's position, which mirrors a firm's value and attitude toward the IT function. The capability can also be improved when attention is raised to the executive level, as managing information security risks needs coordination across all functions. In addition, the effectiveness of information security management is largely determined by the leadership of top management (McFadzean et al. 2007). An IT executive can also affect the believability or organizational commitment to their security strategies (Thong et al. 1996), which in turn enhances a firm's initiatives for managing risks. Finally, given the compensation structure of the top management team, we can observe a firm's attitude toward different functions and their relative importance, which indirectly implies the effectiveness of information security management.

This study has the following limitations. First, this study does not consider executives' individual backgrounds, such as education, experience in information systems, political backgrounds, and cultural differences. These idiosyncratic factors can also affect individuals' risk propensity and capabilities. Second, we do not capture the organizational structure of the executives, such as the reporting structure (e.g., whether the IT executive reports to the CEO), which could also affect an executive's decisions. Last, we do not take into account the monetary losses or the total number of records compromised, as the information is not always available.

Numerous future research avenues exist. By obtaining more detailed individual characteristics of executives, we could investigate how security breaches potentially affect the quality of staffing. It may be worthwhile to examine how the reporting structure in an organization affects the strategic decisions, which in turn affect the effectiveness of information security management. Specifically, the reporting relation between the CIO and CFO or COO as opposed to the CEO has been of interest to practitioners and researchers alike. Due to the reporting requirements of data breach notification laws, the total number and types of records compromised are becoming more readily available. These data could eventually be used to estimate the total amount of losses in a particular security breach, which can be an indication of the severity of the breach. Additionally, the career paths of IT executives and non-IT executives could be of interest. If the recent trend of bringing in IT executives from areas outside of IT continues, it would be interesting to examine if the nature of the associations change. Similarly, if we see non-IT executives begin to come from the ranks of IT units, we might also expect to see some changes in the nature of such associations. We could certainly shed new light on how the IT governance structure affects the severity of information security breaches.

REFERENCES

Aggarwal, R. K., and A. A. Samwick. 1999. Executive compensation, strategic competition, and relative performance evaluation: Theory and evidence. *Journal of Finance* 54 (6): 1999–2043.

Anderson, R. J. 2001. *Why Information Security Is Hard—An Economic Perspective*. Proceedings of the 17th Annual Computer Security Applications Conference, Cambridge, U.K.

Archambeault, D. S., F. T. DeZoort, and D. R. Hermanson. 2008. Audit committee incentive compensation and accounting restatements. *Contemporary Accounting Research* 25 (4): 965–992.

Bloom, M. 1999. The performance effects of pay dispersion on individuals and organizations. *Academy of Management Journal* 42 (1): 25–40.

Bussey, J. 2011. Has time come for more CIOs to start reporting to the top? *Wall Street Journal* (May 17).

Campbell, K., L. Gordon, M. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11 (3): 431–448.

Carpenter, M. A., and J. B. Wade. 2002. Micro-level opportunity structures as determinants of non-CEO executive pay. *Academy of Management Journal* 45 (6): 1085–1103.

Carpenter, M. A., and W. G. Sanders. 2002. Top management team compensation: The missing link between CEO pay and firm performance? *Strategic Management Journal* 23 (4): 367–375.

Chen, D. Q., D. S. Preston, and W. D. Xia. 2010. Antecedents and effects of CIO supply-side and demand-side leadership: A staged maturity model. *Journal of Management Information Systems* 27 (1): 231–272.

Computer Security Institute (CSI). 2011. *CSI Computer Crime and Security Survey 2010/2011*. New York, NY: Computer Security Institute.

Demsetz, H., and K. Lehn. 1985. The structure of corporate ownership: Causes and consequences. *Journal of Political Economy* 93 (6): 1155–1177.

Dhillon, G., and J. Backhouse. 2001. Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal* 11 (2): 127–153.

Dumagan, J., and G. Gill. 2002. Industry-level effects of information technology use on productivity and inflation. In *Digital Economy 2002*, edited by J. Mayer and L. Price, 31–40. Washington, DC: U.S. Department of Commerce.

Eisenhardt, K. M. 1989. Agency theory: An assessment and review. *Academy of Management Review* 14 (1): 57–74.

Ettredge, M. L., and V. J. Richardson. 2003. Information transfer among Internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71–82.

Fiss, P. C. 2006. Social influence effects and managerial compensation evidence from Germany. *Strategic Management Journal* 27 (11): 1013–1031.

Galbraith, C. S., and G. B. Merrill. 1991. The effect of compensation program and structure on SBU competitive strategy: A study of technology-intensive firms. *Strategic Management Journal* 12 (5): 353–370.

Gibbons, R., and K. J. Murphy. 1992. Optimal incentive contracts in the presence of career concerns: Theory and evidence. *Journal of Political Economy* 100 (3): 468–505.

Greene, W. H. 2003. *Econometric Analysis*. Upper Saddle River, NJ: Prentice Hall.

Hall, J. A., and S. L. Liedtka. 2005. Financial performance, CEO compensation, and large-scale information technology outsourcing decisions. *Journal of Management Information Systems* 22 (1): 193–221.

Hallock, K. F. 1997. Reciprocally interlocking boards of directors and executive compensation. *Journal of Financial and Quantitative Analysis* 32 (3): 331–344.

Holthausen, R. W., D. F. Larcker, and R. G. Sloan. 1995. Business unit innovation and the structure of executive compensation. *Journal of Accounting and Economics* 19 (2): 279–313.

ISACA. 2012a. *COBIT 5 for Information Security*. Rolling Meadows, IL: ISACA.

ISACA. 2012b. *Securing Sensitive Personal Data or Information Using COBIT 5*. Rolling Meadows, IL: ISACA.

IT Governance Institute (ITGI). 2005. *Board Briefing on IT Governance*. Rolling Meadows, IL: The IT Governance Institute.

Johnson, A. M., and A. L. Lederer. 2010. CEO/CIO mutual understanding, strategic alignment, and the contribution of IS to the organization. *Information and Management* 47 (3): 138–149.

Kannan, K., J. Rees, and S. Sridhar. 2007. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12 (1): 69–91.

Kearns, G. S., and A. L. Lederer. 2003. A resource-based view of strategic IT alignment: How knowledge sharing creates competitive advantage. *Decision Sciences* 34 (1): 1–29.

Kohli, R., and S. Devaraj. 2003. Measuring information technology payoff: A meta-analysis of structural variables in firm-level empirical research. *Information Systems Research* 14 (2): 127–145.

Li, C., J. Lim, and Q. Wang. 2007. Internal and external influences on IT control governance. *International Journal of Accounting Information Systems* 8: 225–229.

Luftman, J. 2000. Assessing business-IT alignment maturity. *Communications of the Association for Information Systems* 4: Article 14.

Luftman, J., and R. Kempaiah. 2008. Key issues for IT executives 2007. *MIS Quarterly Executive* 7 (2): 99–112.

McFadzean, E., J. N. Ezingeard, and D. Birchall. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review* 31: 622–660.

Oliver, R. L., and E. Anderson. 1994. An empirical test of the consequences of behavior- and outcome-based sales control-systems. *Journal of Marketing* 58 (4): 53–67.

Pavlou, P. A., H. G. Liang, and Y. J. Xue. 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly* 31 (1): 105–136.

Pfeffer, J., and N. Langton. 1993. The effect of wage dispersion on satisfaction, productivity, and working collaboratively: Evidence from college and university faculty. *Administrative Science Quarterly* 38 (3): 382–407.

Posthumus, S., and R. von Solms. 2005. A responsibility framework for information security. *Security Management, Integrity, and Internal Control in Information Systems* 193: 205–221.

Preston, D. S., D. Chen, and D. E. Leidner. 2008. Examining the antecedents and consequences of CIO strategic decision-making authority: An empirical study. *Decision Sciences* 39 (4): 605–642.

PricewaterhouseCoopers (PwC). 2011. *Corporate Directors Increasing Their Focus on Executive Compensation, Risk Management and Succession Planning*. New York, NY: PwC.

Santaló, J., and C. J. Kock. 2009. Division director versus CEO compensation: New insights into the determinants of executive pay. *Journal of Management* 35 (4): 1047–1077.

Smaltz, D. H., V. Sambamurthy, and R. Agarwal. 2004. *The Antecedents of CIO Role Effectiveness in Organizations: An Empirical Study in the Healthcare Sector*. Proceedings of the Conference on Information Systems and Technology, Denver, CO.

Strassmann, P. A. 1994. CIOs should get back to basics. *Datamation* 40 (18): 70–72.

Thong, J. Y. L., C. S. Yap, and K. S. Raman. 1996. Top management support, external expertise and information systems implementation in small businesses. *Information Systems Research* 7 (2): 248–267.

Vafeas, N. 1999. Board meeting frequency and firm performance. *Journal of Financial Economics* 53 (1): 113–142.

Vafeas, N. 2005. Audit committees, boards, and the quality of reported earnings. *Contemporary Accounting Research* 22 (4): 1093–1122.

Wallace, L., H. Lin, and M. A. Cefaratti. 2011. Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems* 25 (1): 185–211.

Wang, T., and C. Hsu. 2010a. *The Impact of Board Structure on Information Security Breaches*. Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Taipei, Taiwan.

Wang, T., and C. Hsu. 2010b. *The Composition of Top Management Team on the Effectiveness of Information Security Management*. Proceedings of the Americas Conference on Information Systems (AMCIS), Buenos Aires, Argentina.

Wang, T., and C. Hsu. 2012. *Board Composition and Operational Risk Events of Financial Institutions*. Working paper, University of Hawaii at Manoa and National Taiwan University.

Wang, T., J. Rees, and K. Kannan. 2012. *The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities*. Working paper, University of Hawaii at Manoa and Purdue University.

Wang, T., K. Kannan, and J. Rees. 2012. The association between the disclosure and the realization of information security risk factors. *Information Systems Research* (forthcoming).

Wilkin, C. L., and R. H. Chenhall. 2010. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24 (2): 107–146.

Yayla, A., and Q. Hu. 2008. *Determinants of CIO Compensation Structure and Its Impact on Firm Performance* Proceedings of the 41st Hawaii International Conference on System Sciences, Big Island, Hawaii.

APPENDIX A

Variable Definitions

Variables	Definition	Value	Source
Breach	A dummy variable indicating whether a firm has reported information security breach. *Breach* equals 1 if a firm has at least one security breach up to *t*, 0 otherwise.	1 or 0	DataLossDB, LexisNexis, CNET, ZDNet
ITEXE	A dummy variable indicating whether there is an IT executive in the top management team. *ITEXE* equals 1 if a firm has an IT executive in its top management team, 0 otherwise.	1 or 0	ExecuComp
ITINT	IT intensity, which is the ratio of annual IT capital to the number of full-time employees at the four-digit SIC code level deflated by the average ratio of all industries.	continuous	BEA
ROA	Return on assets, which equals the net income before extraordinary items and discontinued operations divided by total assets, then multiplied by 100.	continuous	ExecuComp
FTE	Full-time employee, which is the logarithm of the total number of full-time employees.	continuous	Compustat
EPS	Earnings per share, which equals net income minus preferred dividends divided by the weighted outstanding common shares.	continuous	ExecuComp
DPS	Dividends per share, which equals total dividends paid out over a fiscal year.	continuous	ExecuComp
BM	The number of board meetings held during the fiscal year.	continuous	ExecuComp
Turnover	The number of IT executive turnovers in a certain year.	continuous	ExecuComp
Age	IT executive's age at the end of year *t*.	continuous	ExecuComp

(continued on next page)

APPENDIX A (continued)

Variables	Definition	Value	Source
Tenure	IT executive's tenure at the end of year *t*.	continuous	ExecuComp
Firmvol	Standard deviation of the firm's daily stock returns over the past 60 months.	continuous	ExecuComp
TotComp	Total compensation, which is the logarithm of the summation of salary, bonus, stock awards, and stock options.	continuous	ExecuComp
BeComp	Behavior-based compensation, which is the logarithm of salary.	continuous	ExecuComp
OutComp	Outcome-based compensation, which is the logarithm of the summation of bonus, stock awards, and stock options.	continuous	ExecuComp
Distance	Compensation differences of total compensation between IT and non-IT executives, which equals IT executive's compensation minus the average of non-IT executives' compensation.	continuous	ExecuComp
BeDistance	Compensation differences of behavior-based compensation between IT and non-IT executives, which equals IT executive's compensation minus the average of non-IT executives' compensation.	continuous	ExecuComp
OutDistance	Compensation differences of outcome-based compensation between IT and non-IT executives, which equals IT executive's compensation minus the average of non-IT executives' compensation.	continuous	ExecuComp
Sales	Logarithm of sales revenues.	continuous	Compustat

Note that if time is not specified, it represents year *t*–1.