Do the Roles of the CEO and CFO Differ when it comes to Data Security Breaches?

Full Paper

Jacob Haislip
University of North Texas
Jacob.Haislip@unt.edu

Jee-Hae Lim
University of Waterloo
jh2lim@uwaterloo.ca

Robert Pinsker
Florida Atlantic University
rpinsker@fau.edu

Abstract

Using a sample of S&P 1500 firms from 2005-2013, we investigate the independent relationships of Chief Executive Officer (CEO) IT expertise, Chief Financial Officer (CFO) IT expertise, and board level technology committees with data security breaches. Overall, our results indicate that firms that either employ a CEO with IT expertise or implement a technology committee are more likely to detect and report breaches. Further, firms that employ a CFO with IT expertise are less likely to report a breach, suggesting that these firms are better at preventing breaches. The aggregate findings build on the extant corporate governance and risk management literatures.

Keywords

Data Security Breaches, IT Expertise, CEO, CFO, Board Level Technology Committees.

Introduction

According to a recent Ponemon Institute (2015) study, US firms report the highest average cost per breach at $15 million. Further, cyberattacks are costlier the longer they are not detected and accounted for. Ponemon reports an average of 46 days at a cost of $21,155 per day to resolve a detected cyberattack. From a regulatory perspective, the Securities and Exchange Commission (SEC) has felt the need to build on its initial 2011 cybersecurity disclosure guidance by providing an increasing number of comment letters to firms. In multiple instances, the SEC has identified inadequate firm disclosure of data security breach risk and required improved risk disclosure in the following Form 10-K or 10-Q (Rood 2015). Thus, there is a need to change the traditional corporate governance structures to better address the risks and costs associated with data security breaches. The key ideas are that 1) senior management should possess the necessary technical skills to work with the board of directors (henceforth, the "board") to address the risks of data security breaches and 2) a separate board-level technology committee should be established to handle cybersecurity and other information technology (IT) risks. Consequently, the purpose of this study is to investigate the roles that the following three governance actors play in preventing and detecting data security breaches: Chief Executive Officers (CEO) possessing IT expertise; Chief Financial Officers (CFO) possessing IT expertise; and board-level technology committees.

Our study's purpose focuses on the IT governance (ITG) component of the larger corporate governance construct.[1] The principles, policies, and frameworks model set forth by COBIT 5 (ISACA 2013) identifies the board, the CEO, and CFO as necessary elements to define governance objectives and enterprise values. More specific to a cybersecurity context, the following opening statement from a recent National Association of Corporate Directors (NACD) meeting supports the importance of the board and management representing key governance actors needing to effectively communicate with each other, "proper preparation for a security breach begins with board and management discussing how they will handle a breach." (NACD, 2014, 4). Whereas the extant literature has examined our context of data security breaches in general (e.g., Gwebu et al. 2013), technology committees and breaches (Higgs et al. 2016), and CEO IT expertise in a financial reporting context (e.g., Haislip et al. 2016a), no study that has come to our attention considers the importance and role of all three governance actors in firms' cybersecurity strategies.

Using a propensity score matched approach, our sample consists of 265 treatment (breach) firms and 265 control (non-breach) firms from 2005-2014. Firms with reporting data security breach(es) have ITG governance actors with weaker IT expertise. Consistent with our expectations, results indicate that both a CEO with IT expertise and a separate, board-level technology committee are positively associated with reporting a breach, while CFOs with IT expertise are negatively associated with reported breaches. The negative association for CFOs suggests that those with IT expertise are more adept at putting effective internal control policies and procedures into place to prevent breaches from occurring.

In aggregate, our study makes multiple contributions to the governance and risk management literatures. First, we document the complementary roles IT expertise has at the CEO and board levels when detecting and reporting security breaches. Prior related research investigates potential CEO expertise associations with annual disclosure quality and finds evidence suggesting IT expertise provides a benefit financial expertise does not. Second, our related findings should be of interest to academics interested in the associations between board dynamics and risk factors in general and, more specifically, board-level solutions to security breaches. Finally, our findings add to the budding CFO expertise literature. Little is known about the CFO's roles within the firm outside of various financial reporting aspects identified in the respective Finance and Financial Accounting literatures. Despite a plethora of arguments from industry suggesting positive effects of tech savvy CFOs reducing IT risk in general (data security breaches more specifically), and Sambamurthy and Zmud's (2012) conceptual linkage of CFOs to demand-side IT risk management activities in general, no academic research came to our attention empirically linking these two concepts. Further, by investigating CEOs and CFOs separately, we avoid the limitation in prior top executive research that combines the two as "senior management" results (e.g., Li et al. 2007; Hsu and Wang 2015).

Literature Review and Hypothesis Development

A strong IT tone at the top is a common thread between the relevant ITG and IT risk management literatures. Sambamurthy and Zmud's (2012) seminal work is a comprehensive description of IT risk, IT risk management, and ITG. According to the authors, regardless of how judiciously a firm moves forward with its security policies and procedures, it remains exposed to many IT risks (p. 2). Further, firms are digitally-exposed once their security barriers have been breached with intruders using new tactics that are increasingly difficult to prevent or detect. Although the TMT literature has long recognized that strong leadership is a foundational block found in top IT risk management firms, it was not until the recent large number of high-profile security breaches that has made absence of such leadership at the top conspicuously evident (Roboff 2016).

CEOs oversee firm-wide IT policies and strategies to set the strategic IT tone at the top that include such decisions as how risk of security breaches should be assessed, monitored, and mitigated. Masli et al. (2016) contend that CEOs are treated differently by the board than CFOs at least partly due to their

[1] ITG is defined by Debreceny (2013, 129) as "the process by which organizations seek to ensure that their investment in information technology facilitates strategic and tactical goals." According to Higgs et al. (2016), it represents an increasingly important subset of the broader corporate governance environment.

fiduciary duties. Specifically, the authors claim the CEO's duty is of a general nature to ensure the strategic IT flexibility of the firm (p. 7). From a governance perspective, a recent CyLab governance report indicates boards are looking for assurances that their IT risk decisions are based on well thought out and executed strategic IT plans (PR Newswire 2012). These three governance actors, CEOs, CFOs, and the board, and their roles with regard to the security breach aspect of IT risk are discussed next.

CEO IT Expertise

CEOs set the tone for their firms. Their attitudes and decisions affect decision making made throughout multiple levels of the firm (Berson et al. 2008). Further, there is evidence that the background of the CEO can affect their managerial decisions (Bamber et al. 2010; Baik et al. 2011). Haislip and Richardson (2016) find that CEOs with IT expertise improve the information environment for their firms as evidenced by more accurate earnings forecasts. Haislip et al. (2016a) find that firms that report IT-related material weaknesses in internal controls are more likely to hire a CEO with IT expertise following the revelation of the weakness. Finally, Haislip et al. (2016b) find that CEOs with IT expertise disclose key filings more timely than other firms. More relevant to our study, firms that employ a CEO who is comfortable with technology tend to find that the comfort level with IT permeates throughout the firm (Bassellier et al. 2003; Finney and Corbett 2007).[2] Further, a tone of acceptance of IT set by a CEO with IT expertise improves the information environment for the firm.

In aggregate, the findings above agree with the earlier IT risk management discussion and suggest that by setting a strong, strategic IT tone at the top, trickling down to an improved information environment at an operational level, CEOs with IT expertise should be able to improve monitoring effectiveness throughout their firms. Therefore, our first hypothesis is as follows:
H1: The presence of CEOs possessing IT expertise is positively associated with the likelihood of reported breaches.

Technology Committees

The rapid ascension of technology committees is summarized in the 2015 Spencer Stuart Board Index for S&P 500 firms. The existence of technology committees in S&P 500 firms went from 0 in 2000, to 2% in 2002, 7% in 2012, and 9% in 2015 (Spencer Stuart 2015). Kickenweiz et al.'s (2016) interview of public firm board members provides some additional insights for this ascension. Specifically, boards are ill-prepared for the pace of IT developments within their firms. Board members cannot use standard Enterprise Risk Management (ERM) procedures to identify data security risks and most are not IT experts; therefore, their understanding lags reality with regard to IT trends. Further, Kickenweiz et al. (2016) argue that having IT experts in a technology committee is a great advantage, because they can educate the rest of the board about cybersecurity risks.

A recent Protiviti (2016) survey on cybersecurity indicates that in addition to management's policies, the strength of a firm's cybersecurity measures largely falls on board engagement. The study's opening quotation suggests that the Director of the NACD believes forming a technology committee is the correct model for firms to be engaged in cybersecurity oversight. To extrapolate further on this suggestion, he believes that board oversight, in general, is seriously challenged in its ability to review, monitor, and govern data security-related risks (NACD 2015). In their ITG chapter, Sambamurthy and Zmud (2012) make analogous lack of IT expertise comments, while also advocating for a separate, board-level technology committee to serve as a foundation for oversight of critical IT risk decisions.[3]
The presence of a technology committee is an indicator of a strong IT tone at the top. Specifically, firms with technology committees are willing to absorb the costs of another board-level committee in order to

[2] According to PwC's Global CEO Survey (2015b), CEOs see cybersecurity-related technologies as a top-three most strategically important type of digital methodology for their firm.

[3] Similarly, Hines et al. (2015) relate the increased demand for board-level risk management caused by the financial crisis to the formation of risk committees.

improve IT risk oversight. The additional oversight serves as a proxy for active engagement in ITG and IT risk management activities. According to Haislip et al. (2016b), the presence of a technology committee can help monitor and support management's strategic choices related to the utilization of the firm's IT, resulting in an improved information environment. In sum, anecdotal and academic research suggest that firms having dedicated technology committees will provide a strong IT tone at the top such that they are more likely than others to detect and report security breaches. Consequently, our next hypothesis is stated:
H2: The presence of a board-level technology committee is positively associated with the likelihood of reported breaches.

CFO IT Expertise

CFOs typically control the most sensitive firm information on a daily basis; however, until recently CFOs have not been viewed as a critical member of a firm's security team (Durbin 2015). That view is changing according to the results from a 2015 Gartner/Financial Executives Institute (FEI) survey. CFOs now have a major influence over many IT decisions, because the pervasiveness of technology has caused it to be part of firms' business decisions (Gartner 2015). A significant change in the survey results over 2014's survey is the rise of security as the second most critical investment CFO's make in IT. This change is due in large part to some CFOs becoming more tech savvy. A CFO lacking IT expertise representing a weak IT tone at the top can be detrimental to this process, because (s)he does not understand the important issues to report to the board or appropriate questions to ask. A recent Deloitte (2014) survey finds 74% of CFOs view cybersecurity as a high priority, but more than half cite anxieties related to data security and related communications to the board due to lack of expertise.

However, CFOs are typically concerned with regulatory compliance (Burchill 2015) due to their fiduciary duties. The Securities and Exchange Commission (SEC) has recently warned firms that it would be looking into their cybersecurity preparedness to ensure the firms have specific policies and procedures in place to conduct periodic risk assessments (Abromovitz 2014). The SEC examinations specifically involve key ITG metrics including evaluating data security risks and involvement of senior managers and boards of directors (ThinkAdvisor 2015). Further, the Financial Industry Regulatory Authority (FINRA) has recently expressed concern that firms are not acting "reasonably" when it comes to cybersecurity-related policies and practices (Leonhardt 2015). Recent events like the Target, JP MorganChase, and Sony breaches serve as reminders to CFOs of the significant damage to firm reputation and increased CFO turnover if they do not maintain a strong IT security infrastructure (as part of a strong IT tone at the top). The CFO serves a major ITG oversight role with the firm. (S)he is a liaison between the IT department and the board on cyber-related issues and, therefore, needs to understand where the firm's information is at all times and how it is protected from unauthorized access (Katz 2016).

The arguments made by the anecdotal literature cited above are generally supported in academic research by Haislip et al. (2016a), who find that CFOs with IT expertise are more effective than other CFOs at improving internal control environments following IT related material weaknesses. However, as Masli et al. (2016) point out, CFOs are disproportionately punished by the board (i.e., higher turnover relative to CEOs) when IT material weaknesses are reported.[4] Whereas, CEOs typically set the long-term, IT firm strategies in order to detect situations when other managers/employees circumvent firm policies and controls, CFOs are more on the "front line" with regard to preventing security breaches (Bailey et al. 2014). Therefore, consistent with arguments made in the anecdotal, academic ITG, and IT risk management literatures, we predict that CFOs with IT expertise should foster a strong IT tone at the top and put into place security-related control policies that prevent breaches. Our third hypothesis is as follows:
H3: The presence of CFOs possessing IT expertise is negatively associated with the likelihood of reported breaches.

[4] Similar to Masli et al. (2016), in untabulated analysis we find that CFOs are disproportionately punished by the board following breaches. Specifically, we find that CFOs are more likely to experience turnover than CEOs in the year of a reported breach.

Method

Sample and Variable Composition

Following prior research (Gwebu et al. 2013; Higgs et al. 2016), we identify breaches using privacyrights.org. Privacyrights.org identifies 634 reported breaches from 362 firms from 2005 through March, 2014. We then match these identified breaches with our S&P 1500 sample, and end with 127 reported breaches of S&P 1500 firms during the period 2005 through 2013. After eliminating observations with missing data from Compustat, CRSP, and Audit Analytics used to calculate the variables in our models, we arrive at a final sample of 9,633 firm-year observations.

We measure CEO and CFO IT expertise following Lim et al. (2013) and Haislip and Richardson (2016). We first identify the CEOs and CFOs in our sample firms using the Corporate Library. Then, we read the biographies of these executives found using the Corporate Library, Bloomberg, BusinessWeek, or Forbes to determine if the executive has IT expertise. An executive is considered to have IT expertise if they have an academic degree in Computer Science, Electrical Engineering, or Information Systems; or if they previously served in an IT-related position of employment (e.g., Chief Information Officer (CIO), Chief Technology Officer, Vice President of Information Technology, or IT consultant). One author and two research assistants were independently involved in the coding process. The percentage of agreement (the inter-rater reliability) among these four independent coders was over 90% for the *IT Expert* variable respectively. These agreement scores are well above the recommended threshold of 70% (Cohen 1960). Our sample identifies 676 (554) firm-year observations where a CEO (CFO) with IT expertise is employed. Consistent with Higgs et al. (2016), to examine the board's role in ITG, we identify board-level technology committees (*Tech Comm*) using Audit Analytics and find committees with the word "technology" in them. We then manually verify the existence of these committees by reading the annual proxy statements. Our sample identifies 230 firm years in which a technology committee is present.

Research Design

We investigate the likelihood of security breaches for all of our hypotheses. We use the following logistic regression to test the hypotheses:

$$Breach_{i,t} = \alpha_0 + \alpha_1[\text{IT Governance}]_{i,t} + \alpha_2 CIO_{i,t} + \alpha_3 LnAT_{i,t} + \alpha_4 ROA_{i,t} + \alpha_5 Loss_{i,t} + \alpha_6 Leverage_{i,t} + \alpha_7 Weak_{i,t} + \alpha_8 Zscore_{i,t} + \alpha_9 Big4_{i,t} + \alpha_{10} Foreign_{i,t} + \alpha_{11} Merger_{i,t} + \alpha_{12} Extra_{i,t} + \varepsilon_{i,t.} \quad (1)$$

For this model we include year and industry fixed effects, and we estimate robust standard error clustered by firm (Petersen 2009). *Breach* is an indicator variable coded as one if the firm reports a security breach in year t, and zero otherwise. ITG is a representation of our three variables of interest (*CEO IT Expert, Tech Comm,* and *CFO IT Expert*) as explained in the Sample and Variable Composition section. CEOs with IT expertise and technology committees should serve monitoring roles as their ITG role. We predict that these governance actors aid in the detection and reporting of security breaches. Therefore, we expect a positive and significant coefficient on *CEO IT Expert* and *Tech Comm*. CFOs with IT expertise are more likely to play a different role in ITG and should aid in the prevention of breaches. Thus, we expect the coefficient on *CFO IT Expert* to be negative and significant. Following Higgs et al. (2016), we include control variables for other possible determinants of breaches. First, we include *CIO*, because a company employing an IT executive may mitigate the likelihood of a security breach. Next, we include measures of size (*LnAT*), as recommended earlier in this study, and performance (*ROA, Loss, Leverage,* and *Zscore*), because as Higgs et al. suggest larger more successful firms are more attractive targets for potential breaches. We also include *Weak, Foreign, Merger,* and *Extra*, because firms with weak internal control environments or more complicated operational structures may be more susceptible to breaches. Finally, we include *Big4* as these high quality auditors tend to serve as external monitors for their client firms.

Endogeneity Consideration

We also conduct a Heckman (1979) two stage approach to address potential endogeneity concerns. We follow Haislip and Richardson (2016) and use the following probit model shown to predict that likelihood to employ our governance actors:

$$[\text{IT Governance}]_{i,t} = \Omega_0 + \Omega_1 LnAT_{i,t} + \Omega_2 ROA_{i,t} + \Omega_3 Leverage_{i,t} + \Omega_4 High\ Tech_{i,t} + \Omega_5 CIO_{i,t} + \Omega_6 ITMW_{i,t} + \Omega_7 EarnVol_{i,t} + \Omega_8 Foreign_{i,t} + \Omega_9 Merger_{i,t} + \Omega_{10} Restruct_{i,t} + \Omega_{11} ProdcutDiff_{i,t} + \Omega_{12} CostLeader_{i,t} + \Omega_{13} Transform_{i,t} + \varepsilon_{i,t.} \quad (2)$$

Compared to equation (1), there are a few instrumental variables included in this model (*High Tech, ITMW, EarnVol, Restruct, ProductDiff,* and *CostLeader*) that are not associated with *Breach*. We then use the output from this calculation to calculate the inverse Mills ratio separately for each ITG variable and include it in logistic model equation 1. We expect to find the same results using this method as we do in the primary logistic regression.

Results

Table 1 presents a univariate analysis of our variables, comparing the group of *Breach* observations to non-*Breach* observations. It appears that for most variables, the two groups are similar. However, the *Breach* group appears to be larger, less likely to report a loss, more leveraged, report a lower *Zscore,* use less of a cost leader strategy, and report more volatile earnings. Some of these results are not surprising. As discussed earlier in the study, larger and more successful firms tend to more attractive targets for potential breaches. We include all of these variables as control variables in our testing.

	N = 127	**N = 9,506**	**Difference**	**P-Value**
IT Expert CEO	0.094	0.07	0.025	0.28
IT Expert CFO	0.031	0.058	-0.026	0.205
Tech Comm	0.039	0.024	0.016	0.25
CIO	0.15	0.122	0.028	0.338
LnAT	9.509	7.642	1.866	0.000***
ROA	0.056	0.049	0.007	0.465
Loss	0.087	0.149	-0.062	0.051*
Leverage	0.618	0.498	0.12	0.000***
Weak	0.031	0.044	-0.012	0.508
Zscore	3.858	4.677	-0.819	0.063*
Big 4	0.961	0.924	0.036	0.122
Foreign	0.331	0.394	-0.064	0.144
Merger	0.228	0.23	-0.002	0.961
Extra	0.031	0.017	0.014	0.228
Restructure	0.441	0.488	-0.047	0.288
ITMW	0.008	0.008	0	0.98
ProductDiff	0.144	0.098	0.046	0.293
CostLeader	0.957	1.13	-0.173	0.011**
EarnVol	1089.26	232.1	857.158	0.000***

Table 1. Univariate Analysis

Empirical Results

Table 2 presents the results from logistic regression model (1) in which we investigate the effects of *IT Expert CEO, Tech Comm,* and *IT Expert CFO* on the likelihood of a reported breach. All of the models are estimated using robust standard errors clustered by firm, with a sample time frame from 2005-2013. All of the columns include year and industry fixed effects. The dependent variable for all of the columns is

Breach, which is an indicator variable coded as one if the firm reports a security breach in the current year, and zero otherwise.

As predicted, the coefficient on *IT Expert CEO* is positive and significant ($p < 0.10$) in both Columns (1) and (4), suggesting that firms that employ CEOs with IT expertise are more likely to detect and report breaches. This result supports H1 and suggests that CEOs with IT expertise positively influence the strategic IT tone at the top and effectively monitor IT security. As predicted in H2, we find that the coefficient on *Tech Comm* is positive and significant ($p < 0.01$) in Columns (2) and (4). This result suggests that firms who have a board-level technology committee are more likely to detect and report breaches even if the firm employs CEOs and/or CFOs with IT expertise. According to Turel and Bart (2014), high levels of board participation in ITG activities, regardless of existing IT needs, increases firm performance. Therefore, we conduct an F-Test to determine if technology committees are more effective than CEOs with IT expertise at reporting breaches. As shown at the bottom of Table 4, we find that the two coefficients are not statistically significantly different from each other. Next, the coefficient on *IT Expert CFO* is negative and significant ($p < 0.10$) in both Columns (3) and (4), suggesting that firms that employ CFOs with IT expertise are more likely to prevent security breaches. This result supports H3. Turning to the control variables, it is not surprising that *LnAT* is positive and significant, because larger firms tend to be targets for breaches. We then consider the potential interplay among our three governance actors by interacting *Tech Comm* with both *IT Expert CEO* and *IT Expert CFO*. We find that there are no reported breaches for any firms that have a technology committee and either an IT expertise CEO (15 observations) or IT expertise CFO (25 observations). The findings from these small samples provide some evidence suggesting that firms employing two of our governance actors are successfully preventing breaches.

		(1)	(2)	(3)	(4)
	Pred	*Breach*	*Breach*	*Breach*	*Breach*
IT Expert CEO	+	0.529*			0.574**
		(0.060)			(0.048)
Tech Comm	+		1.056***		1.080***
			(0.006)		(0.007)
IT Expert CFO	-			-0.766*	-0.813*
				(0.072)	(0.063)
CIO		-0.003	-0.011	0.016	-0.031
		(0.992)	(0.971)	(0.959)	(0.919)
LnAT		0.743***	0.749***	0.745***	0.752***
		(0.000)	(0.000)	(0.000)	(0.000)
ROA		-0.693	-0.656	-0.707	-0.527
		(0.574)	(0.587)	(0.576)	(0.661)
Loss		-0.123	-0.093	-0.107	-0.079
		(0.774)	(0.828)	(0.801)	(0.852)
Leverage		1.014***	0.971***	0.993***	0.994***
		(0.003)	(0.004)	(0.004)	(0.003)
Weak		0.037	0.072	0.064	0.058
		(0.941)	(0.885)	(0.898)	(0.908)
Zscore		0.030	0.037	0.039*	0.030
		(0.212)	(0.129)	(0.094)	(0.208)
Big4		-0.558	-0.569	-0.543	-0.574
		(0.259)	(0.251)	(0.276)	(0.256)
Foreign		-0.211	-0.192	-0.210	-0.241
		(0.413)	(0.452)	(0.413)	(0.345)
Merger		-0.244	-0.279	-0.221	-0.269

	(0.302)	(0.232)	(0.351)	(0.253)
Extra	0.232	0.223	0.202	0.198
	(0.625)	(0.638)	(0.670)	(0.677)
Constant	-11.130***	-11.143***	-11.149***	-11.217***
	(0.000)	(0.000)	(0.000)	(0.000)
Year Indicators	Included	Included	Included	Included
Industry Indicators	Included	Included	Included	Included
Observations	9,633	9,633	9,633	9,633
Psuedo R2	0.196	0.198	0.197	0.201
Model X^2	288.830***	285.420***	294.470***	291.730***

Table 2. The Effect of Executive Expertise and Tech Committees on Security Breaches

Table 3 presents the results of our Heckman Model. The columns in this table mirror those presented in Table 2, except these include the inverse Mills ratio (*Mills*) calculated in equation (2). The inverse mills ratio is calculated separately for each of our variables of interest, and therefore, we are unable to combine all of the variables into the same model. The results are essentially the same as those presented in Table 4 as all of our variables of interest are significant ($p < 0.10$) and in the predicted direction. These results suggest that even after controlling for endogeneity, we find that firms that utilize CEOs with IT expertise and technology committees are more likely to detect and report security breaches, and that firms employing CFOs with IT expertise are effective in preventing security breaches.

		(1)	(2)	(3)
	Pred	*Breach*	*Breach*	*Breach*
IT Expert CEO	+	0.575*		
		(0.054)		
Tech Comm	+		1.124***	
			(0.004)	
IT Expert CFO	-			-0.730*
				(0.083)
CIO		-0.062	0.079	-0.001
		(0.839)	(0.826)	(0.998)
LnAT		0.737***	0.748***	0.783***
		(0.000)	(0.000)	(0.000)
ROA		-1.355	-0.609	0.518
		(0.176)	(0.635)	(0.756)
Loss		-0.512	-0.286	-0.245
		(0.265)	(0.556)	(0.606)
Leverage		1.637***	1.062***	0.950***
		(0.000)	(0.003)	(0.009)
Weak		0.045	0.124	0.128
		(0.928)	(0.803)	(0.796)
Zscore		0.044**	0.037	0.039*
		(0.029)	(0.143)	(0.109)
Big4		-0.678	-0.606	-0.575
		(0.161)	(0.221)	(0.251)
Foreign		-0.489**	-0.192	-0.275
		(0.038)	(0.455)	(0.291)
Merger		-0.274	-0.120	-0.159
		(0.253)	(0.678)	(0.504)
Extra		0.140	0.054	-0.064
		(0.781)	(0.921)	(0.908)
Mills		-0.435	0.303	1.181***
		(0.215)	(0.326)	(0.007)
Constant		-9.718***	-12.152***	-13.715***
		(0.000)	(0.000)	(0.000)
Year Indicators		Included	Included	Included
Industry Indicators		Included	Included	Included
Observations		9,633	9,633	9,633

Psuedo R2	0.153	0.198	0.199
Model X^2	169.330***	316.820***	320.070***

Table 3. Heckman Model

Conclusion

Security breaches are costly for firms who are feeling pressure from stockholders and regulators to make improvements to their ITG structure to prevent and detect said security breaches. Our study takes an IT tone at the top/IT risk management perspective to investigate three governance actors to see if they are effective in the fight against security breaches. Qualitative analysis suggests that S&P 1500 firms are increasingly recognizing the value of IT expertise of CEOs and technology committees, especially, given their numbers essentially double over the course of our sample period.

Although our study is subject to the typical data-related limitations, we also cannot rule out the possibility that the positive associations found essentially represent firms who are breached more because they possess CEOs with IT expertise or technology committees. Our consistent results related to the Heckman Model testing help to curb this possibility, but future research should go a step further and investigate our research question using a causation model. Our study is also limited to primarily large, public firms, because they typically command more attention. Future research should examine our variables of interest using all public firms to investigate any potential firm size issues.

REFERENCES

Abromovitz, L. 2014. "Cybersecurity prep: What the SEC's looking for." (http://www.financial-planning.com/30-days-30-ways).

Baik, B., Farber, D. and Lee. S. 2011. "CEO ability and management forecasts," *Contemporary Accounting Research* (28:5), pp.1645-1668.

Bailey, T., Kaplan, J., and Rezek, C. 2014. Why senior leaders are on the front line against cyberattacks. *Elevate(*http://www.elevateconsult.com/why-senior-leaders-are-the-front-line-againstcyberattacks/).

Bamber, L., Jiang, J. and Wang. I. 2010. "What's my style? The influence of top managers on voluntary corporate financial disclosure," *The Accounting Review* (85:1), pp.1131-1162.

Bart, C., and O. Turel. 2009. The role of the board in IT governance: Current and desired oversight practices. *International Journal of Business Governance and Ethics* (4:4), pp. 316-329.

Bassellier, G., Benbasat, I., and Reich, H. (2003). "The influence of business managers' IT competence on championing IT," *Information Systems Research* (14:4), pp. 317- 336.

Bell, T. 2015. "How not to get fired as a CISO." (http://www.csoonline.com/article/3000854/it-careers/how-to-not-get-fired-as-ciso.html).

Berson, Y., Oreg, S., and Dvir, T. 2008. "CEO values, organizational culture and firm outcomes," *Journal of Organizational Behavior* 29: 615-33.

Burchill, J. A. 2015. "For CFOs, cybersecurity risk is like an iceberg," (http://ww2.cfo.com/cyber- security-technology/2015/07/cfos-cybersecurity-risk-like-iceberg/).

Cohen, J. 1960. "A coefficient for agreement for nominal scales," *Education and Psychological Measurement* (20:1), pp. 37-46.

Debreceny, R. 2013. "Research on IT governance, risk, and value: Challenges and opportunities," *Journal of Information Systems* (27:1),pp. 129-135.

Deloitte. 2014. "CFO Signals." (http://www2.deloitte.com/us/en/pages/finance/articles/cfo-signals-program-survey-finance-priorities-company.html.

Durbin, S. 2015. The CFO's role in cybersecurity. (http://ww2.cfo.com/accounting-tax/2015/03/cfos role-cyber security/).

Finney, S. and Corbett, M. (2007). "ERP implementation: a compilation and analysis of critical success factors," *Business Process Management* (13:3), pp. 329-347.

Gartner. 2015. "Survey analysis: Critical CFO technology needs: 2015 Gartner FEI study." (https://www.gartner.com/doc/3114318/survey-analysis-critical-cfo-technology).

Gwebu, K., Wang, J., and Wang, L. 2013. "Data security breach impact and disclosure." In *proceedings of the American Accounting Association Annual Meeting*, Anaheim, CA.

Haislip, J., Masli, Z., A., Richardson, V. ., and Sanchez, J. M. 2016a. "Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades," *Journal of Information Systems* (30:1), pp. 41-70.

Haislip, J., Karim, K., Lin, K. J., and Pinsker, R. 2016b. "The influences of CEO IT expertise and board-level technology committees on disclosure timeliness," In *proceedings of* the *Accounting Information Systems Midyear Meeting*, Houston, TX.
Heckman, J. 1979. "Sample selection bias as a specification error," *Econometrica* (47:1), pp. 153-161.
Higgs, J., Pinsker, R., Smith, T., and Young, G. 2016. "The relationship between board-level technology committees and reported security breaches," *Journal of Information Systems,* forthcoming.
Hines, C. S., Masli, A., Mauldin, E. G., and Peters, G. F. 2015. "Board risk committees and audit pricing," *Auditing: A Journal of Practice & Theory* (34:4), pp. 59-84.
Hsu, C., and Wang, T. 2015. Composition of the top management team and information security breaches. In the *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. M. M. Cruz-Cunha and I. M. Portela, Eds. IGI Global, pp: 116-134.
ISACA. 2013. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA.
Karamanou, I. and Vafeas,N. 2005. "The association between corporate boards, audit committees, and management forecasts: An empirical analysis," *Journal of Accounting Research (43*:3), pp. 453-486.
Katz, D. M. 2016. "Cyber risk demands all hands on deck: Proofpoint CFO." (http://ww2.cfo.com/cyber-security-technology/2016/02/cyber-risk-demands-hands-deck-proofpointcfo/).
Kickenweiz, B., Sedlock, G., and Daum, J. H. 2016. "Technology in the boardroom: Five things Directors should be thinking about." (https://www.spencerstuart.com/research-and-insight/technology-in-the boardroom-five-things-directors-should-be-thinking-about.
Kobelsky, K., Richardson, V. J., Smith, R. E., and Zmud, R. W. 2008. "Determinants and consequences of firm information technology budgets," *The Accounting Review (83:*4), pp. 957-995.
Leonhardt, M. 2015. Regulators say firms need 'reasonable' data safeguards. (www.wealthmanagement.com).
Li, C., Lim, J-H., and Wang, Q. 2007. "Internal and external influences on IT control governance," *International Journal of Accounting Information Systems* (8:4), pp. 225-239.
Lim, J-H., Stratopoulos, T. C., and Wirjanto, T. 2013. "Sustainability of a firm's reputation for IT capability: Role of senior IT executives," *Journal of Management Information Systems* (30:1), pp. 57-96.
Masli, A., G., Peters, Richardson, V. J., and Sanchez, J. M. 2010. "Examining the potential benefits of internal control monitoring technology," *The Accounting Review (85:*3), pp. 1001-1034.
Masli, A., Richardson, V. J., Watson, M. W., and Zmud, R. W. 2016. Senior executives' IT management responsibilities: Serious IT-related deficiencies and CEO/CFO turnover. *MIS Quarterly* (forthcoming).
National Association of Corporate Directors. 2014. "Advisory council on risk oversight: Summary of proceedings." (https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=12849).
Petersen, M. 2009. "Estimating standard errors in finance panel data sets: Comparing approaches," *Review of Financial Studies* (22:1), pp. 435-480.
Ponemon Institute. 2015. "2015 cost of cyber crime study: Global." (http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/).
PR Newsire. 2012. "Top executives say GRC programs must better align to strategic priorities to meet board needs: RSA convenes top corporate leaders in governance, risk management, security and compliance at inaugural RSA Archer GRC executive forum." July, 5 pages.
Protiviti. 2016. "Arriving at internal audit's tipping point amid business transformation." (https://www.protiviti.com/en-US/Documents/Surveys/Infographic-2016-Internal-Audit-Capabilities-and-Needs-Survey-Protiviti.pdf).
PwC. 2015a. "Governing for the long term: Looking down the road with an eye on the rear-view mirror." (www.pwc.com/us/ACDS2015).
PwC. 2015b. 18th annual global CEO survey. (www.pwc.com/ceosurvey).
Rood, J. L. 2015. Handling cybersecurity disclosures: Practical tips for when and what to disclose. *Accounting Today*. (http://www.accountingtoday.com/news/audit-accounting/handling-cybersecurity-disclosures-74418-1.html).
Sambamurthy, V., and Zmud, R. W. 1999. "Arrangements for information technology governance: A theory of multiple contingencies," *MIS Quarterly* (23:2), pp. 261-290.
Sambamurthy, V., and R. W. Zmud. 2012. *Guiding the Digital Transformation of Organizations,* Tallahassee, FL: Legerity Digital Press.
Spencer Stuart. 2015. "Spencer Stuart U.S. Board Index 2015." (https://www.spencerstuart.com/~/media/pdf%20files/research%20and%20insight%20pdfs/ssbi-2015_110215-web.pdf?la=en).
ThinkAdvisor. 2015. "SEC to launch second round of cyber exams, issues risk alert." (www.Thinkadvisor.com/2015/09/15).
Turel, O., and Bart, C. 2014. "Board-level IT governance and organizational performance," *European Journal of Information Systems* 23, pp. 223-239.