Too Busy to Monitor? Board Busyness and the Occurrence of Reported Information Security Incidents

Carol Hsu
Tongji University, China
carolhsu@tongji.edu.cn

Tawei (David) Wang
DePaul University, USA
david.wang@depaul.edu

Abstract

This paper investigates the association between board busyness (i.e., directors with multiple positions) and the occurrence of reported information security incidents. Building on prior studies of board busyness, this paper argues that directors holding multiple board seats may fail to commit the time and effort necessary to ensure the appropriate information security strategy or investment plans are in place. Our results demonstrate that board busyness is positively associated with reported information security incidents. This effect is larger when independent directors are busy, thus suggesting the importance of the governance role played by independent directors in managing information security risks. The board of directors' role has been emphasized in anecdotal evidence and IT governance frameworks, but our study empirically demonstrates the board's relevance in information security strategy and management.

1. Introduction

In the information security literature, the imperative role of top management to support the adoption and implementation of information security management has received well-acknowledged support [19, 21]. Nonetheless, with the increasing headlines reporting on data breaches and cyberattacks, there is a call that board-level information security governance assess information technology (IT)-related risks that can potentially have a catastrophic impact on organizational performance and operations [26, 33]. Anecdotal evidence from, for example, Deloitte, Ernst & Young (EY), and the International Association of Privacy Professionals (IAPP) highlights the board of directors' importance regarding information security strategy and the potential damage to organizational performance in the event the board fails to perform its job of risk oversight. Additionally, in late 2013, the US retailer Target experienced one of the largest data breaches in the industry, resulting in the resignation of the company's chief executive officer (CEO) and a call from Institutional Shareholder Services (ISS) to oust several of Target's directors on the board for their failure to ensure the appropriate management of information security risks. These developments are consistent with the message from the IT Governance Institute [23] claiming that boards of directors now bear a greater responsibility in ensuring the protection of information assets in organizations and establishing an appropriate governance strategy to meet the strategic business objectives and comply with regulatory compliance requirements.

Given the importance of board-level governance for IT issues, emerging scholarly research develops a conceptual framework for board members' role in IT governance [8, 37] or empirically investigates the effect of board-level IT governance on both directors' perceived organizational, financial performance [44] and reported security breaches [20]. Turel and Bart [44] note that the board of directors is responsible for overseeing the management of an organization by "asking management questions about existing and potential IT risks" and "making sure risks are identified and monitored" (p.225). This perspective highlights the board of directors' important organizational capability of endorsing security policy and ensuring the appropriate countermeasures are established against security risks.

In this research, we claim that the board plays a crucial role in influencing how senior managers plan risk mitigation strategies and develop proactive cybersecurity practices. To further understand the board's role in security governance, for the following reasons, this study extends the focus from the board structure to the concept of board busyness, which commonly refers to the number of multiple board appointments a director holds that consequently renders him/her too busy to adequately perform the monitoring function. Our perspective on busyness is rooted in the argument that limited attention capabilities and time constraints prevent a busy director from effectively performing the monitoring function. Although Ferris, Jagannathan, and Pritchard [15] find no evidence of a negative association between multiple board appointments and corporate

URI: https://hdl.handle.net/10125/71372
978-0-9981331-4-0

performance, Fich and Shivdasani [16] question the methodological design in Ferris, Jagannathan, and Pritchard [15], and their reexamination of empirical data indicates that multiple directorships are associated with weaker corporate governance. Fich and Shivdasani [16] finding is consistent with the policy recommendation from the National Association of Corporate Directors [43] that called for limits on the number of board seats held by directors. Jiraporn et al. [25] also find that busy directors have a higher tendency to be absent from board meetings. Thus, from the viewpoint of time allocation and monitoring, we argue that busy directors holding multiple board seats may fail to provide the time commitment required to participate in the company's overall security strategy and governance.

Second, Curry [8] posits that, in contrast with their understanding of other forms of risks, most board members do not possess expertise in cybersecurity risks; to overcome this obstacle, the recommendation is that the board actively engage in conversations with security leaders in the organization and include information security discussions in its meeting agenda. Additionally, as highlighted in a PricewaterhouseCoopers report, "boards can keep up to speed with effectiveness of the company's security program by meeting regularly with the company's top security owner, such as the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO)" (2015, p.1). Again, these viewpoints imply that effective information security governance requires the board's commitment and efforts to engage in a management discussion, to understand the risk profile specific to its organization, to set the direction for risk management and security policy, and to monitor the information security program's effectiveness. Overall, we believe that, in addition to board composition, board busyness is another feature that is highly relevant and worthy of investigating in the security governance context.

Thus, our research objective is to empirically investigate the link between board busyness and the effectiveness of organizational information security. Similar to prior studies, we used the information security incidents report as an indicator for measuring the effectiveness of information security management [29]. Empirically, reported information security incidents were manually collected from DataLossDB , while board busyness was calculated using the eigenvector centrality measure in the network analysis. We also perform additional analyses by focusing on (1) the role of independent directors and (2) the source of the information security incidents.

The paper is organized as follows: The next section reviews the existing literature on information security management and governance and the relevant theoretical background on board busyness and governance effectiveness. Section three presents our econometric model and research methodology. Next, we discuss the empirical results and conclude the paper with the theoretical and practical implications of this research.

2. Theoretical background and hypothesis development

In the first part of this section, we review and discuss the extant studies on information security management and governance. In particular, we focus on studies addressing the role of top management and the board in the design and implementation of information security programs. In part two, we discuss the association between board busyness and information security governance, followed by the development of the main hypotheses for our empirical analyses.

2.1. Information security management and governance

Within the literature, the primary focus has been placed on organizational end users and employees, such as user awareness and motivation [9, 27], information security policy compliance [5, 46, 49], and risk management [42]. In recent years, attention has also been shifted to the importance of top management in directing and shaping the implementation and consequences of information security management. From our perspective, studies such as [18, 21, 36] are significant because they demonstrate the importance of top management's character in supporting the implementation of information security programs in an organization and shaping employees' attitudes toward information security compliance. Nonetheless, from the information security governance perspective, the board of directors is another key group of actors who must understand the business risks and ensure they are adequately addressed. Their importance has been gradually reported and highlighted in a broader concept of IT governance, of which information security governance and risk management are an integral part [32, 34]. Nolan and McFarlan [33] were among the first to highlight the value of board oversight of IT investment strategy and corporate information asset risk management. Building on their early work on the IT strategic grid, Nolan and McFarlan [33] proposed that companies in different modes of the strategic grid should implement diverse

arrangements for board committees and their corresponding responsibilities. For example, companies in factory strategic modes require that their boards of directors conduct regular reviews of security effectiveness and reliability to avoid possible business interruptions and organizational crises. Nolan and McFarlan [33] suggest that these companies' boards should question both the quality of business continuity planning against attack and the quality of management processes for ensuring a 24/7 service level. Andriole [1] also conducted a descriptive survey with more than fifty CIOs and found that CIO perception of board oversight for IT investment and project management is relatively low. Andriole [1] offers prescriptive recommendations for actions to increase board members' level of engagement as well as the alignment of business and IT strategy at the board level. Turel and Bart [44] also determine that board-level involvement in IT governance can influence organizational performance. They conclude that board-level IT governance is an important organizational capability for achieving strategic advantages and managing IT-associated risks. A similarly positive relationship between board IT governance and firm performance was also reported in studies by both Jewer and McKay [24]and Turel, Liu, and Bart [45].

Emphasizing the concept of information security governance, Johnston and Hale [26] illustrate the discrepancy of information protection quality between those companies that implemented information security governance and those that did not. They found that for those organizations with information security governance in place, the reported executive management's support is much higher. Parent and Reich [34] propose a framework of IT risk governance chain and dashboard to help the board more effectively govern IT-related risks such as infrastructure, information, and business continuity risks. Hsu and Wang [20] drew on the organizational demography perspective and conducted an exploratory study on the association between board structure and composition, such as board size, the heterogeneity of directors' ages/tenures, and the possibility of security breaches. Hsu and Wang [20]indicate that security breaches are less likely to occur when the board is larger and the directors, on average, are older and possess longer organizational tenures.

Overall, we find that the value and importance of board oversight of IT investment and security management have been widely recognized and discussed in practitioner-oriented publications and surveys [23, 41]. To address this gap, we next theorize and empirically test board busyness and its impact on information security breaches in organizations.

2.2. Board busyness and information security management effectiveness

Studies on upper management examine a variety of factors that might influence its effectiveness in performing these functions (e.g., the board's composition). In our empirical research, we focus on another important feature called board busyness. As we briefly note in the introduction, multiple directorships can pose implications for the allocation of time and attention to effectively perform the monitoring function. Harris and Shimizu [17] explain that busy boards are "likely to threaten available preparation time for board meetings…time constraints may limit these directors' ability to provide useful advice" (p. 777). We find this argument particularly salient in the information security governance context. When compared with general financial and managerial controls, this dimension of security knowledge is more organization specific [48] and requires that the board "be aware of the organization's information assets and their criticality to ongoing business operations" (p.21) [23]. Rothrock, Kaplan, and Van der Oord [40] propose that the board involvement in cybersecurity discussion should not go beyond the yearly or semiannual reporting meetings. Namely regarding nontechnical board members that comprise the board's majority, spending more time interacting with information security officers can greatly increase the knowledge and awareness of possible IT-related risks and breaches, which is consistent with Parent and Reich's [34] argument that the boards should devote more time and effort to IT risk governance than they have in the past.

Thus, increased board awareness implies greater demand from the board's time for gaining a clear and full understanding of protecting corporate information assets and asking relevant questions about technology risks and current security practices. Further, increased board awareness might lead to an increase in the number or length of board meetings to allow for access to organizational knowledge. Jiraporn et al. [25] demonstrate that directors with more board seats have a greater tendency to be absent from board meetings. We believe such absences may pose implications for accessing organization-specific information that might be available during board meetings and may thus weaken the soundness of information security governance in a firm. Thus, we propose the following hypothesis.

Hypothesis 1: Board busyness is negatively associated with the effectiveness of information security management.

The corporate governance literature has also emphasized the distinction between independent

directors and insider directors. Scholars argue the independent director's role is particularly important for enforcing the monitoring and oversight function of organizational performance [11, 28, 38]. Independent directors are more likely to have independent perspectives because they are outside directors rather than employees of or affiliated with the firm. Beasley [2] found a negative relation between the incidence of financial fraud and independent directors, while other studies have provided empirical support for the adverse impact on firm performance when outside/independent directors hold multiple board seats. For instance, Fich and Shivdasani [16] discovered that, when a majority of outside directors are busy holding three or more board seats, firms have weaker corporate governance. Additionally, Falato, Kadyrzhanova, and Lel [13] suggests that investors do value independent directors' efforts and time in governance oversight and that independent directors' busyness is negatively related to firm value. Similarly, Liu, Wang, and Wu [30] found that independent directors' attendance at board meetings plays an important role in investor protection.

In the information security context, we contend that independent directors would be serving a more important function than insider directors in terms of monitoring the strategic position and implementing the information security program within an organization. Turel and Bart [44]also indicate that "the board can raise IT questions…and ultimately prevent opportunistic behaviors of management (e.g., ensure that the executive management team invests in proper IT security measures, rather than giving themselves a bonus)" (p. 227). However, aligning with our earlier argument on the time and attention required to gain familiarity with the cybersecurity practices in an organization, we argue that, when independent directors serve on multiple boards, there exist greater implications for the board's decision quality in providing direction and oversight for information security programs compared to the board as a whole. Accordingly, we propose the following hypothesis.

Hypothesis 2: The negative association between the busyness of independent directors and the effectiveness of information security management is greater than that for the board as a whole.

3. Data description and econometric model

For our empirical analysis, we collected data regarding reported information security breaches, board busyness, and control variables. Please note that we only consider information security incidents reported by news articles, but not incidents detected by companies.

3.1. Dependent variable

Our study operationalized the effectiveness of information security management by using the realization of information security risks (i.e., reported information security incidents) because (1) the effectiveness of information security management is not observable by both insiders and outsiders [29] and (2) this approach has been commonly used in information security-related studies [29, 50] and operational risk management studies [47]. We collected reported information security breaches (denoted as *BREACH*) that were reported as information security incidents in news articles. *BREACH* is a dummy variable that equals one when a firm-year has reported information security breaches and zero otherwise. Specifically, we manually collected all reported information security incidents from DataLossDB (http://datalossdb.org/) including those from 2003 to 2013 in order to match what we have access for the board data. DataLossDB is operated by a nonprofit organization and states on its website that it collects breach information daily from news outlets including news feeds, blogs, and websites. For our analyses, we excluded the information security breaches of nonprofit organizations, government agencies, and firms that are not publicly traded. The information security incidents collected based on the above steps were all confidential.

3.2. Independent variable

We used the standard eigenvector centrality measure [3, 4, 12] from the network analysis to capture board busyness for each firm in our sample. Specifically, we used the measure to capture a network of firms through multi-position directors—those who hold positions on the boards of multiple firms. The eigenvector centrality measure is a comprehensive measure commonly used for a nondirectional network. Our measure is different from the average number of director positions held by all directors used in prior studies [15, 16] because we believe this method more appropriately captures how busy the board is both directly and indirectly. To calculate this measure, we gathered board information from the RiskMetrics database from 2003 to 2011. We only collected data up to 2011 due to data access limitations.

Our method assigns a score (eigenvector centrality score) to all vertices (companies) in the network mentioned earlier. A high eigenvector score

means a vertex (a company) is connected to many other companies who also achieve high scores through multi-position directors. That is, the higher the value is, the busier the board of a company is because multi-position directors exist and because other companies wherein a director holds multiple positions also have busy boards of directors. For our analyses, we considered two centrality measures: one calculated based on all a firm's board directors (*NET*), and another calculated based solely on a firm's independent directors (*NET_INDE*).

3.3. Control variables

We controlled the firm's and board's characteristics that have been demonstrated as being related to information security breaches in previous studies. Firm characteristics were gathered from Compustat, while board characteristics were collected from RiskMetrics. We considered firm size, performance, and growing opportunities for firm characteristics; firm size (*SIZE*) refers to the number of employees (in thousands). Previous studies [48] argue that, although larger firms may possess more effective control mechanisms regarding information security management than smaller firms, they may also be more likely to be targeted. We further control for performance and growing opportunities, the former of which was defined as return-on-assets (*ROA*, net income of the firm divided by total assets) and the latter of which was captured through the market-to-book ratio (*MB*, market value of the firm divided by the common stockholders' equity). For board characteristics, we considered board size (*N_DIR*), percentage of independent directors (*P_INDE*), the heterogeneity of directors' ages (*SD_AGE*), and the heterogeneity of directors' tenures (*SD_TENURE*). Board size, measured as the number of directors on the board, has been considered to be correlated with information security breaches because the board may (1) monitor the effectiveness of the firm's information security management programs [22] and/or (2) guide the development and implementation of information security strategies [22]. In addition, previous studies [10] have reported that a nonlinear association may exist between board size and the effectiveness of information security management. Accordingly, in our analyses, we additionally consider the square of the board's number of directors (*N_DIRSQ*). Independent directors are involved in corporate governance mechanisms and may ensure that information security risks are appropriately accounted for, which would reduce the possibility of information security incidents [14]. In our analyses, we controlled for the percentage of independent directors on the board. The heterogeneity of the directors' ages is measured by the age variation coefficient, which equals the standard deviation of all directors' ages divided by the average age of all the firm's directors. The heterogeneity of the directors' tenures is also measured by their variation coefficient (i.e., the number of years directors have worked for the firm), which equals the standard deviation of all directors' tenures divided by the average tenure of all the firm's directors. The heterogeneity of the directors' ages and tenures may potentially affect the effectiveness of a firm's risk management [47]. Finally, year and industry effects were also controlled.

We then merged the following three sets of data: information security incidents, board connectedness, and control variables. The resulting sample size is 11,642 firm-event observations; among these, 11,387 firm-event observations lack information security events, while 255 firm-event observations possess information security incidents. This rare event characteristic is consistent with what previous studies identified [48]. We then reperformed our analyses using a matched sample in the section entitled Additional Analyses.

3.4. Econometric model

We tested our hypotheses with Equation (1), which was estimated using the logistic regression model after controlling for industry- and year-fixed effects with a firm's clustered standard errors [35].

$$BREACH = \beta_0 + \beta_1 Busyness + \beta_j \text{Control} + \Sigma\text{Year} + \Sigma\text{Industry} + \varepsilon \quad (1)$$

Busyness represents either *NET* or *NET_INDE*, while Control represents the control variables defined earlier.

4. Empirical results

4.1. Main findings

The year and industry breakdowns show that more reported information security incidents in recent years and more incidents for industries with one-digit SIC codes "5" (wholesale and retail trade), "6" (finance, insurance, and real estate), and "7" (services). The descriptive statistics of the variables show that, on average, comprises nine board directors (*N_DIR*) wherein approximately 75% are independent directors (*P_INDE*). The firm size (*SIZE*), on average, is approximately 19,000 employees. For firms with and without reported information security incidents, all variables are significantly different at a 1% level. Specifically, firms without reported security incidents

have a lower level of centrality (i.e., the directors are less busy), fewer directors (*N_DIR*), fewer independent directors (*P_INDE*), and are smaller in size (*SIZE*). No large correlations that may affect our analyses were observed.

The main results are provided in Table 1, wherein four models based on Equation (1) reveal how our results may vary with the inclusion or exclusion of variables. Please note that the year- and industry-fixed effects are included although not reported in Table 1, and all significance levels are two-sided. Model (1) only considers the association between board busyness (*NET*) and the occurrence of information security breaches (*BREACH*). The result demonstrates that board busyness (*NET*) is positively associated with *BREACH* (coefficient = 6.855, p < 0.01), suggesting that, when the firm's board is busier (i.e., when the board member holds more positions), the likelihood of information security incidents increases based on our logistic regression model (Greene 2012).

Model (2), Model (3), and Model (4) consider board busyness with board characteristics and, in Model (4), additional control variables. The results indicate that board busyness (*NET*) is significantly and positively associated with the likelihood of information security incidents (3.412, $p < 0.01$); that is, when the board member is busier (i.e., she/he holds more positions), the log-odds of having a breach increase by approximately 3.412. Similarly, board busyness as measured by independent directors (*NET_INDE*) is also positively associated with the possibility of information security breaches (2.728, $p < 0.01$); that is, when the independent board members are busier, the log-odds of having a breach increase by approximately 2.728. Specifically, and as we discussed earlier, information security risk is idiosyncratic to individual firms [48]. To more effectively manage information security risks, a thorough understanding of IT resources, operations, and the firm's specific needs is required. From this viewpoint, busy directors, although they may be equipped with industry knowledge and possess a broader understanding of emerging threats, may not devote enough effort to a specific firm, which may hinder the effectiveness of information security management as captured by reported information security incidents in our analyses. The findings consistently demonstrate that larger firms (*SIZE*) are more likely to experience reported information security breaches. In addition, board size (*N_DIR*) is positively associated with the possibility of information security breaches (coefficients = 0.470 and 0.486, respectively, $p < 0.05$). Such findings suggest that larger boards may be less effective in communicating and coordinating, which subsequently affects the effectiveness of information security management. However, this is not a linear association (the squared term, *N_DIRSQ*, is -0.019, $p < 0.05$); the nonlinear association suggests that either a relatively small or large board is more effective in managing information security risks than is a medium-sized board. We discuss our main results in the next section.

Table 1. Main Regression Results

	Model (1)	Model (2)	Model (3)	Model (4)
Intercept	-3.667***	-7.453***	-7.501***	-7.105***
	(-10.52)	(-6.46)	(-6.40)	(-6.04)
NET	6.855***	3.412***		
	(12.61)	(4.30)		
NET_INDE			2.728***	3.418***
			(2.76)	(4.00)
N_DIR		0.470**	0.486**	0.540***
		(2.51)	(2.53)	(2.63)
N_DIRSQ		-0.019**	-0.019**	-0.021**
		(-2.19)	(-2.09)	(-2.22)
P_INDE		0.293	0.363	-0.437
		(0.39)	(0.47)	(-0.60)
SD_AGE		-0.049	-0.059*	-0.056
		(-1.41)	(-1.70)	(-1.50)
SD_TENURE		-0.040	-0.044	-0.040
		(-1.28)	(-1.40)	(-1.39)
SIZE		0.010***	0.010***	0.009***
		(7.49)	(7.95)	(6.79)
ROA				-1.303
				(-1.24)
MB				0.028
				(0.93)
N	11,642	11,642	11,642	10,852
Pseudo R^2	0.16	0.21	0.20	0.20

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.10$ (two-tailed test), *z* statistics are in parentheses and are estimated with firm clustered standard errors as in Petersen (2009). All models include industry- and year-fixed effects, although the results are not presented.

4.2. Additional analyses

In this subsection, we first consider whether board busyness is related to reported information security breaches with different sources of the incident (i.e., whether the reported information security incident is caused by insiders or outsiders). Untabulated findings demonstrate that, when the reported breach is caused by insiders, the association between board busyness (*NET*) is significantly larger than when it is caused by outsiders (i.e., 3.345 vs. 2.893, $\chi^2 = 106.93$, $p < 0.01$),. We also discuss this result in the following section.

We further investigate whether our results are affected by governance or high-technology industries. For governance, it is possible a firm with a stronger governance environment is less likely to be affected by board members' busyness. To examine this possibility, we gathered the governance score from Bloomberg and reperformed our analyses. The findings are consistent with our expectation.

Regarding high-tech companies, information security management is more inherent to their business operations. For high-tech companies, a busy board may have a smaller impact on information security management than other industries. To reperform our analyses, we employed Chemmanur, Loutskina, and Tian [7] definition claiming high-tech industries are the companies in the following three-digit SIC codes: 357, 366, 367, 372, 381, 382, and 384. Our results are consistent with our expectations.

Additionally, we consider the following diverse settings of our model to further validate our results. First, busy boards may be endogenous. However, choosing the appropriate instrumental variables is challenging because (a) prior studies lack clear guidance, (b) most firm characteristics are theoretically related to both board business and information security to some extent, and (c) many firm characteristics have mixed associations with information security breaches. Accordingly, we choose total assets and industry membership as our instrumental variables in the first stage. Specifically, total assets and industry membership may be indicators of a busy board, but they are not clear indicators of information security breaches from a theoretical perspective. In addition, total assets are not highly correlated with existing size measures (number of employees; correlation coefficient = 0.48). Given that we cannot find strong instrumental variables for the first stage from a theoretical perspective, we rely on a statistical test for weak instruments. The first-stage model is estimated by the ordinary least squares model, while the second-stage model remains the logistic regression model. In particular, the test first demonstrates that we reject the weak instrument hypothesis ($\chi^2 = 27.32$, $p < 0.01$). In addition, the partial R^2 and F-statistic equal 0.08 and 15.52 ($p < 0.01$), respectively, further suggesting the instrumental variables are not weak. The main results remain similar and thus further validate our main analysis.

Second, we consider performance and growing opportunity as additional control variables, for which our main results remain similar. Third, we also use lagged independent variables in our model (i.e., breach is at time $t + 1$, while independent variables are at time t), and our main results remain similar. Fourth, our results may also be affected by a potentially biased sample; that is, firms with a reported security breach may exist in specific industries and may be larger in size. Therefore, we formed a control group using one-to-one propensity score matching with the nearest neighbor algorithm. To achieve this, we first regressed *BREACH* on *SIZE*, industry, and year using a logistic regression model. From the model, the propensity score (conditional probability of having information security breaches) is calculated, the nearest neighbor (control group with the smallest gap of propensity compared to the event group) is identified, and the resulting sample size becomes 491 observations. We then reperformed our analyses and the main results are similar.

In addition to quantitative analyses, we conducted seven interviews—two with senior security consultants who possess extensive experience in information security governance, three with the listed companies' CIOs who reported to the board on IT and cyber security issues, and two with the listed companies' board members—to gain insights concerning the board's role in information security governance and the implication of board busyness. Interviews with practitioners also serve as a method for applicability checks [39, 44]. In the interviews, we briefly described our work and asked interviewees about both their thoughts on the research findings and their personal experiences with or observations of board busyness and information security governance. We coded the interviews based on the role of board in information security governance and in particular, the implications of board busyness on the effectiveness of information security management in organizations.

All our interviewees were consistent in their viewpoints concerning the increasing importance of board involvement in security governance, and one CIO commented, "Continuous organizational investment in technology, employee awareness, training programs and IT professional skills is needed for good organizational security. Without strong support from the board, the security initiatives and investment may suffer when competing with resources with other business growth-driven initiatives."

We also asked our interviewees about the mechanisms through which the board gains familiarity with the firm's security practices. Most interviewees considered engaging in conversations with security experts or CIOs and having security risk management progress reports on board meeting agendas as crucial practices. Speaking from his own experiences working with board members, one senior consultant stressed that, if a board director is busy and misses a board meeting, he or she will miss the opportunity to "understand and ask the right questions about security risks." Interestingly, one CIO from a listed IT company further suggested that the inclusion of cyber security expertise on the board would be the fastest way to educate other board members about information security governance.

To enrich our quantitative findings on the impact of independent directors, we also asked the interviewees to comment on the role of independent directors. One interviewee who serves as an independent director for

a financial company and holds multiple board seats claimed: "To understand IT security risk better, independent directors need to be on both the audit and risk management committees. I believe that the frequency with which these directors attend the meetings can be an important indicator of good governance in organizations. Now, technology affects every aspect of business operations. I would also suggest that independent directors should have a regular dialog with CIOs to understand the security risks in the context of the business operation. I often find these conversations very useful."

In short, we consider that the above qualitative findings extend the support for our argument on the time and attention required for the board to acquire security risk knowledge and to effectively perform the information security monitoring function.

5. Discussion and conclusions

This study has examined the relationship between board busyness and the effectiveness of information security management in organizations. Our findings have demonstrated that, when a board employs directors who hold multiple board seats, the likelihood of reported information security incidents is higher. Furthermore, our results provide evidence of a significant and positive correlation between independent directors' busyness and the possibility of reported information security incidents.

We believe our research findings offer important theoretical contributions to information security strategy and governance research in modern organizations. First, the focus on information security management has been predominantly centered on mechanisms that enforce user compliance and awareness. Among these mechanisms, a number of studies have pointed to the value of top management involvement in and support of the implementation of an information security program [21]. However, to the best of our knowledge, a limited number of studies have examined the relevance of the board of directors in information security strategy and governance. Much of the relevant work is available in practitioner-oriented frameworks or guideline-related publications [22]. In this research, we integrate the practical viewpoints with a theoretical grounding from the corporate governance literature. With this foundation, we extend the notion of top management support to the board level by discussing information security governance. From the standpoint of risk oversight, we draw on the board busyness concept and examine its impact on the effectiveness of information security management in organizations. Our findings help reinforce the practitioner viewpoint by offering evidence of the linkage between board busyness and the likelihood of information security breaches. We believe further quantitative or qualitative studies may be conducted to analyze how interaction and collaboration between the board and management team might strengthen information security governance and oversight. Another interesting study might involve analyzing the impact of board support on employee compliance, attitude, and behavioral intention. Future research may also look into broad IT competency and the effectiveness of information security governance.

In addition, the practical implications of our findings lend support to Nolan and McFarlan's [33] suggestion to establish an IT governance committee work on the role of a board-level technology committee. Our study provides practical guidance to boards and management teams in several ways; for example, Nolan and McFarlan [33] propose that a company should "select appropriate members and the chairman and determine the group's relationship to the audit committee" (p. 8). However, we believe the level of board busyness is a unique contribution to the consideration of board member selection based on this proposal. Our work demonstrates that a busy board member might not have the time and commitment required to understand and evaluate the process of information security planning and implementation. Furthermore, as exemplified in our interviews with practitioners, for effective information security governance, board members must develop organization-specific knowledge and analyze the formal and regular reports from relevant functions. All these endeavors require a greater amount of effort and time. Therefore, other than a board member's technical knowledge, we recommend that, when appointing an IT governance committee, attention should be paid to the number of multiple board appointments a director holds.

Second, our findings can bring research attention to the corporate governance area. Studies in this area have previously focused on the relation between board busyness and organizational performance. Our empirical results highlight that an evaluation of how well the board performs its monitoring and oversight function should not be narrowly confined to the scope of its financial and operational performance. Given advances in technology and regulatory compliance, our study adds a new dimension to the discussion of a board governance's performance and risk management role. We believe our exploratory findings shed new light on how organizations understand and assess the board's value with a broader scope. Furthermore, board member composition studies have indicated the significance of independent directors in

corporate governance and oversight. From the perspective of agency cost, our empirical results offer support to the argument that the independent director is an important mechanism for ensuring organizations have appropriate measures established to react to any threats to corporate information or assets.

Third, our additional analysis offers another interesting and important finding from the perspective of insider and outsider attacks. Previous studies have highlighted the importance of employees' compliance with information security policy, as noncompliance can impose financial costs upon an organization [6]. Our literature review demonstrates that the extant studies have focused on the antecedence or effectiveness of factors that might instigate employees' compliance intentions and behaviors at the employee level [31, 42]. In this research, we raise the level at which this issue is examined by focusing on the value of board oversight in reducing the likelihood of an insider attack. We extend support to the dominant view regarding the board of directors' crucial role in shaping information security culture and call attention to strengthening security governance at the board level for internal security policy compliance.

However, some research limitations exist. First, the completeness of security breach data and director data is limited—a shortcoming we addressed by conducting interviews with practitioners. Second, similar to previous studies, our study is unable to directly capture how a director with multiple positions allocates his/her time and efforts. Future research may employ qualitative case studies to enhance the understanding in different contexts. Third, information security breaches can differ in type and total losses. However, our study is limited to incidents involving confidential information. Fourth, our study is unable to control for firms' security policies and the compliance issues, which may be an important consideration for future studies. Fifth, decisions regarding information security management involve all related parties in an organization, which may be investigated in future studies.

6. References

[1] S. Andriole, "Boards of Directors and Technology Governance: The Surprising State of the Practices," Communications of The Association for Information Systems, 22, ^(24), 2009, pp. 373-394.

[2] M. S. Beasley, "An empirical analysis of the relation between the board of director composition and financial statement fraud," The Accounting Review, October, 1996, pp. 443-466.

[3] P. Bonacich, "Factoring and weighting approaches to clique identification," Journal of Mathematical Sociology, 2, 1972, pp. 113-120.

[4] P. Bonacich, "Power and centrality: A family of measures," American Journal of Sociology, 92, 1987, pp. 1170-1182.

[5] S. Boss, L. Kirsch, I. Angermeier, R. Shingler, and R. Boss, "If Someone is Watching, I'll Do What I'M Asked: Mandatoriness, Control and Information Security," European Journal of Information Systems, 18, ^(2), 2009, pp. 151-164.

[6] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness " MIS Quarterly, 34, ^(3), 2010, pp. 523-548.

[7] T. J. Chemmanur, E. Loutskina, and X. Tian, "Corporate Venture Capital, Value Creation, and Innovation," Review of Financial Studies, 27, ^(8), 2014, pp. 2434-2473.

[8] S. Curry, "Boards Should Take Responsiblity for Cybersecurity. Here's How to Do IT," Harvard Business Review, November, 2017, pp. 1-4.

[9] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, 20, ^(1), 2009, pp. 79-98.

[10] P. de Andres and E. Vallelado, "Corporate governance in banking: The role of the board of directors," Journal of Banking & Finance, 32, 2008, pp. 2570-2580.

[11] G. Drymiotes, "Managerial Influencing of Boards of Directors," Journal of Management Accounting Research, 20, 2008, pp. 19-45.

[12] E. Estrada and J. A. Rodrìguez-Velázquez, "Subgraph centrality in complex networks," Physical Review E7, 2005,

[13] A. Falato, D. Kadyrzhanova, and U. Lel, "Destracted directors: Does board busyness hurt schareholder value?," Journal of Financial Economics, 2014, p. forthcoming.

[14] E. F. Fama and M. C. Jensen, "Agency Problems and Residaul Claims," Journal of Law and Economics, 26, 1983, pp. 327-349.

[15] S. Ferris, M. Jagannathan, and A. Pritchard, "Too Busy to Mind the Business? Mointoring by Directors with Multiple Board Appointments," Journal of Finance, 58, ^(3), 2003, pp. 1087-1111.

[16] E. Fich and A. Shivdasani, "Are Busy Boards Effective Monitors?," Journal of Finance, 61, ^(2), 2006, pp. 689-724.

[17] I. C. Harris and K. Shimizu, "Too Busy To Serve? An Examination of the Influence of Overboarded Directors," Journal of Management Studies, 41, ^(5), 2004, pp. 775-798.

[18] C. Hsu, "Frame misalignment:interpreting the implementation of information systems certification in an organization," European Journal of Information Systems, 18, ^(2), 2009, pp. 140-150.

[19] C. Hsu, J.-N. Lee, and D. Straub, "Institutional Influences on Information Security Innovation," Information Systems Research, 23, ^(3), 2012, pp. 918-939.

[20] C. Hsu and T. Wang, "Exploring the Association between Board Structure and Information Security

Breaches," Asia Pacific Journal of Information Systems, 24, ^(4), 2014, pp. 531-557.
[21] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Role of Top Management and Organizational Culture," Decision Science, 43, ^(4), 2012, pp. 615-660.
[22] ISACA, *COBIT 5 for Information Security*. Rolling Meadows, IL: ISACA, 2012.
[23] IT Governance Institute, "Information Security Governance: Guidance for Boards of Directors and Executive Management," IT Governance Institute 2006.
[24] J. Jewer and K. McKay, "Antecedents and Consequences of Board IT Governance: Institutional and Strategic Choice Perspectives," Journal of the Association for Information Systems, 13, ^(7), 2012, pp. 581-617.
[25] P. Jiraporn, W. Davisdson, P. DaDalt, and Y. Ning, "Too Busy to Show Up? An Analysis of Directors' Absences," The Quarterly Review of Economics and Finance, 49, ^(3), 2009, pp. 1159-1171.
[26] A. Johnston and R. Hale, "Improved Security through Information Security Governance," Communications of ACM, 52, ^(1), 2009, pp. 126-129.
[27] A. Johnston and M. Warkentin, "Fear Appeal and Information Security Behaviors: An Empirical Study," MIS Quarterly, 34, ^(3), 2010, pp. 549-566.
[28] A. Klein, "Audit committee, board of director characteristics, and earnings management," Journal of Accounting and Economics, 33, 2002, pp. 375-400.
[29] J. Kwon, J. Rees, and T. Wang, "The Association between Top Management Involvement and Compensation and Information Security Breaches," Journal of Information Systems, 27, ^(1), 2013, pp. 219-236.
[30] H. Liu, H. Wang, and L. Wu, "Removing Vacnt Chairs: Does Independent Directors' Attendance at Board Meetings Matter?," Journal of Business Ethics, 133, 2016, pp. 375-393.
[31] P. B. Lowry, G. D. Moody, D. F. Galletta, and A. Vance, "The drivers in the use of online whistle-blowing reporting systems," Journal of Management Information Systems, 30, ^(1), 2013, pp. 153-190.
[32] M. Mähring, "The Role of the Board of Directors in IT Governance: A Review and Agenda for Research," in *Americian Conference on Information Systems*, Acapulco, Mexico, 2006.
[33] R. Nolan and F. McFarlan, "Information Technology & the Boards of Directors," Harvard Business Review, 83, ^(10), 2005, pp. 96-106.
[34] M. Parent and B. H. Reich, "Governing information technology risk," California Management Review, 51, ^(3), 2009, pp. 134-152.
[35] M. A. Petersen, "Estimating Standard Errors in Finance Panel Data Sets: Comparing Approaches," Review of Financial Studies, 22, 2009, pp. 435-480.
[36] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Awareness Training: An Action Research Study," MIS Quarterly, 34, ^(4), 2010, pp. 757-778.
[37] W. Raghupathi, "Corporate Governance of IT: A Framework for Development," Communications of ACM, 50, ^(8), 2007, pp. 94-99.
[38] C. G. Raheja, "Determinants of Board Size and Composition: A Theory of Corporate Boards," Journal of Financial and Quantitative Analysis, 40, 2005, pp. 283-306.
[39] M. Rosemann and I. Vessey, "Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks," MIS Quarterly, 32, ^(1), 2008, pp. 1-22.
[40] R. A. Rothrock, J. Kaplan, and F. Van der Oord, "The Board's Role in Managing Cybersecurity Risks," in *Sloan Management Review*, ed: Massachusset Institute of Technology, 2018.
[41] T. Scholtz, "Survey Analysis: Information Security Governance 2012," Gartner, 2012.
[42] J. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," MIS Quarterly, 34, ^(3), 2010, pp. 503-522.
[43] R. B. Stobaugh, *Report of the NACD Blue Ribbon Commission on Director Professionalism*, Washington, D.C.: National Association of Corporate Directors, 1996.
[44] O. Turel and C. Bart, "Board-level IT Governance and Organizational Performance," European Journal of Information Systems, 23, ^(2), 2014, pp. 223-239.
[45] O. Turel, P. Liu, and C. Bart, "Board-Level Information Technology Governance Effects on Organizational Performance: The Roles of Strategic Alignment and Authoritarian Governance Style," Information Systems Management, 34, ^(2), 2017, pp. 117-136.
[46] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," Information & Management, 49, ^(7-8), 2012, pp. 190-198.
[47] T. Wang and C. Hsu, "Board composition and operational risk events of financial institutions," Journal of Banking & Finance, 37, 2013, pp. 2042-2051.
[48] T. Wang, K. Kannan, and J. Rees, " The association between the disclosure and the realization of information security risk," Information Systems Research, 24, ^(2), 2013, pp. 201-218.
[49] C. Yang, K. Ramamurthy, and K. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," Journal of Managment Information Systems, 29, ^(3), 2013, pp. 157-188.
[50] J.-C. Yen, J.-H. Lim, T. Wang, and C. Hsu, "The Impact of Audit Firms' Characteristics on Audit Fees Following Information Security Breaches," Journal of Accounting and Public Policy, 37, ^(6), 2018, pp. 489-507.