Asia Pacific Journal of Information Systems
Vol. 24, No. 4, December 2014 http://dx.doi.org/10.14329/apjis.2014.24.4.531

# Exploring the Association between Board Structure and Information Security Breaches*

Carol Hsu**, Tawei Wang***

Although the area of information security planning and management has gained an increased attention, not much discussion was available on the role and the impact of the board members towards a firm's security management and governance decisions. In this research, we draw on corporate governance and the organizational demography literature to conduct an exploratory empirical study on the association between the board structure of a firm and the possibility of information security breaches. Our results show that the board size, the average age/tenure and the heterogeneity of age could reduce the possibility of security breaches while the proportion of independent directors and the heterogeneity of tenure could increase it. Our findings shed lights on the important role played by the board when managing information security risks in organizations.

Keywords : Information Security, Board Structure, Breach Announcement, Information Security Governance

* The authors would like to thank the review team's constructive feedback that has improved the paper substantially. The authors are also grateful to the financial support from National Taiwan University and the University of Hawaii at Manoa.
** Corresponding Author, College of Management, National Taiwan University
*** School of Accountancy, Shidler College of Business, University of Hawaii at Manoa

# Ⅰ. Introduction

While the advances in, and commoditization of, information communication technology (ICT) enable business organizations to achieve and maintain competitiveness in the marketplace, combating the increasing numbers of external and internal security threats that exploit organizational vulnerabilities is a major challenge [Deloitte, 2009; Richardson, 2008]. Goel and Shawky [2009] indicate that the announcement of security breaches had a negative impact on the market value of the publicly traded firms. Furthermore, the growth in regulatory mechanisms, such as the Sarbanes-Oxley Act (SOX) and Personal Data Protection Act, has also had a profound impact on the discursive process about risk management and corporate governance in organizations. Over the years, we have seen the emergence and inclusion of information security strategy as part of the strategic discussions at the board level. In 2007, 57% of the respondents in the Deloitte Global Security Survey indicated that information security strategy was an important issue for board members. We argue the above statics might underestimate the involvement of board in information security management. From the perspective of regulatory compliance and IT-enabled business operations, the topic of information security and risk management might have been explicitly integrated under the discussion of corporate governance in general. For instance, Sarbanes-Oxley Act Section 404 requires corporation senior management and board of directors to be responsible on the effectiveness of internal control, within which information technology control plays an important role in ensuring the confidentiality, availability and integrity of organizational information. Thus, we contend that the board might not discuss information security strategy as a separate agenda. Instead, information security's content and relevance have often been integrated as part of corporate governance discussion. As the IT Governance Institute[1] report state that

> "boards of directors will increasingly be expected to make information security an intrinsic part of governance" (p. 11).

More and more empirical examples from the industry have offered support to this trend of the development. To name, the recent event of Target's data breach in late 2013, which led to the resignation of CEO and re-election of the company's directors, has shown the awakening recognition on the importance of the directors in safeguarding organizational information assets. In 2014, the National Association of Corporate Directors had nearly 100 board directors attended its first cybersecurity summit. Other companies such as Kellogg and Delta Air Lines have been reported to discuss the cybersecurity issues at their board meetings.

Therefore, against this background, this study attempts to explore the relation between board structure and the likelihood of information security breaches. Within corporate governance literature, scholars have shown that a company's board of directors plays a crucial role in influencing how managers handle risks and develop policies. Studies have shown variables such as board size and heterogeneity can have an im-

1) http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf.

pact on the board's decision-making processes, which in turn might influence the likelihood of fraud [Beasley, 1996] and bankruptcy [Daily and Dalton, 1994], for instance. Following the similar vein, we argue that board structure and heterogeneity might affect the outcome of the decision made on information technology control and information security governance, consequently, affect the effectiveness of information security management in organizations. In this study, our objective is to explore the above association. Nevertheless, scholars have pointed out that the effectiveness of the organization's information security programs can be difficult to observe by both insiders and outsiders. Prior literature often uses information security events to capture the consequences of information security management (e.g., [Kwon et al., 2013; Wang et al., 2012]). We adopt similar approach in this empirical study. In particular, we would like to explore the relation between the board's structure as well as heterogeneity and the likelihood of information security events.

For our empirical analysis, we develop and test our hypotheses using the secondary archival data of S&P 1500 firms in the Risk Metrics database for the period from 1997 to 2009. This database allows us to retrieve information about the board composition such as the number of independent directors on the board, and age as well as tenure of each director. Similar with other studies, we collect media reports on information security breaches from major media outlets using the *Factiva* database as well as the *CNet* and *ZDNet* websites. Our findings demonstrate that the board size, the average age/tenure and the heterogeneity of age are negatively associated with the possibility of security breaches. In contrast, the proportion of independent directors and the heterogeneity of tenure are positively related to the likelihood of security breaches. We believe that our empirical findings have a number of theoretical and practical contributions. First, our research findings can extend support to the emerging industry awareness on the importance of board directors in information security management. This can strengthen the arguments for incorporating information security to a boardroom issue. Second, our empirical results further provide insightful analysis regarding the relationship between the board composition and the likelihood of information security breaches. Literature in corporate governance field has shown board size and other demographic characters can influence the group dynamics and the subsequent decision outcome of the boardroom discussion. Our empirical analysis can be of useful when selecting board of directors, e.g., the re-election of board members at Target in 2014. We consider that with this knowledge, the company would be able to evaluate the issue such as board tenure and heterogeneity. Third, while top management has been known for its importance in information security management, the existing studies overlook the potential role of board of directors in this area. Thus, we consider that our exploratory findings can stimulate further research in the information security field to study different aspects of board composition in managing information security issues in organizations.

The remainder of the paper is organized as follows. In the next section, we consider the theoretical perspectives relevant to an organization's board structure and information security

management policy. In Section 3, we describe our theoretical framework and present our hypotheses. We continue with the description of the research methodology deployed in this study and the discussion of empirical findings in Section 4 and Section 5. In Section 6, we conclude with discussion of the contributions and implications of our research.

## 2. Research Motivation and Theoretical Framework

In this section, we discuss our research motivation and background within the context of information security management and governance.

### 2.1 Organizational Aspect of Information Security Management

As mentioned earlier, the widespread adoption of information technology infrastructure has focused managerial and scholarly attention on one of its unwanted side effects, i.e., the risks associated with technology diffusion (e.g., [Carr, 2003; Ciborra, 2006]). Through our review of the prior literature, we found that the organizational aspect of information security management research is still relatively limited compared with researches on its technical counterpart. Within the organizational perspective, scholars have identified the importance of a company's senior management in determining the information security strategy. Straub and Welke [1998] pointed out that the scope of management knowledge can influence the adequateness and effectiveness of security planning in the organizations; and Chang and Ho [2006] observed that the IT competence of a business manager has a positive influence on information security management. Kankanhalli et al. [2003] posited that strong support from an organization's top management usually results in a greater effort to implement deterrent or preventive controls. More recently, Hsu [2009] concluded that the perception of top management can play an influential role in the roll-out of information security management certification.

In addition to studies of senior management involvement, some researchers have examined the security issues associated with the end-user's behaviour. For instance, D'Arcy et al. [2009] found that user awareness of security countermeasures, such as policy and computer monitoring, is directly associated with the perceived severity and certainty of penalties for IS misuse. Herath and Rao [2009] analyzed the impact of extrinsic and intrinsic motivation on an employee's intention to comply with the organization's IS security policy. Their results demonstrate that extrinsic motivations, such as social influence and peer pressure, are important in determining an individual's intention to comply with such policies. Intrinsic incentives, such as the perceived effect of one's behaviour, also have a positive impact on the intention to comply with security policy. In addition to studies of management and end-user involvement in information security management, some researchers have investigated the economic issues associated with investment in information security management [Cavusoglu et al., 2005; Gordon and Loeb, 2002; Gordon and Loeb, 2006], security policy and certification development [Backhouse et al., 2006; Dhillon and Torkzadeh, 2006; Siponen and Iivari, 2006] and risk management frameworks [Baskerville, 2008; Karabacak and

Sogukpinar, 2005].

In this paper, we recognize the contribution of the above studies to the organizational approach to information security. However, we believe that the strategic importance of effective IS management at the board level is apparent and should be addressed by researchers and practitioners in light of legislative development and significance of IS security governance. We discuss this aspect in the next sub-section.

## 2.2 Information Security Governance

In recent years, calls for more effective information security governance have grown stronger in the practitioner community. With the ever increasing complexity and interconnectivity of technology infrastructure and the corresponding reliance on digitalized information, it is now imperative that information security issues are discussed and addressed at the senior management and board level. To this end, the IT Corporate Institute also released a report containing information security governance guidelines for a company's board of directors and executive management. It clearly defines information security governance as

> "a subject of enterprise governance that provides strategic direction, ensures that objectives are achieved, manage risks appropriately, use organizational resources responsibly, and monitors the success or failure of the enterprise security program." (p.17)

The report highlights the need for senior executives and the board of directors to understand, guide, and prioritize information security management initiatives in an organization. Clearly, support and guidance from the board can have a substantial impact on the effectiveness of an information security program.

Within the scholarly community, several studies have implicitly pointed to the relevance of the board on information security governance. Chai et al. [2011] analyze the relation between the market value and security investment announcements. They found that the investor community overall showed favorable reactions on a firm's security investment decision. Yayla and Hu [2008] investigate the role of a CIO in corporate governance and a firm's performance. In their empirical investigation of 433 companies, the authors found that CIO compensation can suffer from the lack of IT attention at the board level. More importantly, the alignment of CIO and other top management compensation packages has a significant positive effect on a firm's long-term performance. Focusing on security threats and vulnerabilities, Cavusoglu et al. [2004] assess the impact of security breaches on the market value of breached companies. Their results indicate a negative market reaction when there is an Internet security breach announcement. Why are the above findings relevant to the board structure of a firm? In addition to the call for attention from the practitioner community, learning from the management and accounting literature, researchers have highlighted that the corporate boards of directors have a great influence on corporate strategy and performance (e.g., [Baysigner and Butler, 1985; Ellstrand et al., 2002]). Furthermore, as indicated in the Introduction, information technology has been a crucial element of organizational internal control to meet legislative requirements. Putting to-

gether, we argue that the board members have an important role in a firm's information security governance. That is, their decisions will have an extensive implication on the implementation of information technology control and governance decision. As a result, these decisions will reflect on the effectiveness of information security management and the likelihood of information security breaches of a firm. Based on this line of argument, we propose that the issue of corporate board characteristics deserves more attention in the field of information security research. In the next section, drawing on the literature on corporate governance research, we lay the theoretical framework for our empirical investigation.

## 2.3 Theoretical Framework

Corporate governance is one of the mechanisms designed to solve the agency problem. That is, through control and monitoring functions, a firm can lower the interest of conflicts between the owner and the managers [Jensen and Meckling, 1976]. In the corporate governance literature, the design and composition of the board is often discussed because of its oversight and monitoring function of a firm's strategies and structures [Applegate et al., 2009; Baysigner and Butler, 1985; Core et al., 1999; Shleifer and Vishny, 1997; Walsh and Seward 1990). With the authority to select, dismiss and reward important decision-makers in organizations, the board serves the function of monitoring management actions to ensure the protection of stockholders' values in corporations. In evaluating the dynamics and capabilities of the board as an effective control mechanism, the organizational demography literature is popular among researchers. As Bantel and Jackson [1989] explain that

> "the demography argument is relevant in that the decreased communication and increase conflict associated with heterogeneity could influence the decision-making processes and outcomes of top management teams." (p.109)

In addition to the work of Bantel and Jackson [1989], different studies have been published in analyzing the link between demography and firm performance. For instance, Rosenstein and Wyatt [1990] demonstrate a positive stock price reaction around the announcement date of an additional outside director and suggest that shareholder wealth is affected by the proportion of outside directors. Yermack [1996] find that firm performance is a decreasing function of board size because a large board has the problems of poor communication and poor decision-making activities. Other scholarly studies drew attention to the effect on board composition on corporate strategy ranging from impact of strategic planning [Judge and Zeithaml, 1992] to R&D investment strategy [Kor, 2006]. Given that there is no past IS security literature available as well as to be consistent with the prior corporate board demography research (e.g., [Beasley, 1996; Goodstein et al., 1994]), we formulate our hypotheses in the following dimensions : the board size, demographic characteristics of the board, and the proportion of inside/independent directors serving on the board. We detail our hypothesis development below.

*Board Size*: The size of the board is a commonly considered component of board struc-

ture. In accordance with the group dynamic theories, an increase in the number of group members adds opposing values to group performance. While a larger group size brings the benefits of additional resources, it also generates difficulties in control and coordination during the decision-making process [Smith et al., 1994]. With respect to board size, Monks and Minow [1995] have shown that the larger the size of the board, the stronger the control function is and the more knowledge and experience of these directors have to the management team. However, prior evidence also suggests that a large board could result in communication difficulties and make the board ineffective [Jensen, 1993; Lipton and Lorsch, 1992].

In the context of information security, the uncertainty faced by a firm changes rapidly, we also see the tension of increasing board size in determining information security governance approach. From the perspective of knowledge contribution in group decision-making, we believe that the increasing size of the board can contribute to the knowledge base of various security issues, and hence can reduce the possibility of information security breaches. In particular, the development of security technologies and the issues of cybersecurity risks are constantly changing and evolving. Therefore, having a larger board can help the generation of new knowledge and broaden the horizon of understanding in this fast-development area. However, other scholars hold different viewpoints when considering the communicating quality in group decision-making process. Studies have also shown that a larger group of directors can also complicate and slow down the decision-making process at the board meeting [Olson, 1982] and hinder the organization's capability of responding to the environmental change and potential information security threats [Goodstein et al., 1994; Harrison, 1987]. In accordance with this school of thoughts, we consider that have more board members can hinder the effectiveness and quality of decision-making. Since information security issues are more diverse and less defined such as the scope of information security risk disclosure or the level of information security investment, a larger group of directors might lead to a variety of opinions and the difficulties to reach consensus. As a result, a larger size board could make the board less effective and increase the possibility of information security breaches.

Since both theoretical arguments from the literature could be true when applying to the context of information security, we set up two competing hypotheses as in Hypothesis 1a and 1b.

*Hypothesis 1a: The number of the board of directors is positively associated with the likelihood of information security breaches.*

*Hypothesis 1b: The number of the board of directors is negatively associated with the likelihood of information security breaches.*

*The Independence of the Board*: The composition of individuals who serves on the board of the directors can either be internal senior managers or independent members from outside of the organization. Internal manager possesses a greater amount and better quality of information that is relevant to strategic decision. By contrast, the conventional wisdom that supports the value of independent directors normally establishes from the perspective of agency cost or monitoring cost such as Forker [1992], Klein [2002],

Raheja [2005], and Drymiotes [2008]. Proponents argue that independent directors are better monitors to reduce the agency problem faced by the firm (i.e., enhance the monitoring function) which could increase the performance of the firm [Core et al., 1999].

In our information security context, we argue that inside (employee or affiliated) directors compose the internal knowledge about the value and risk associated with the internal operation and business process while outside director offers the experiences and knowledge associated with the emerging risks which might be overlooked by the internal management. We consider that with regard to management of information security, it might require a higher percentage of inside directors for the following reasons. First, as D'Arcy et al. [2009] pointed out, about 50% to 75% of security breaches and the misuse of IS resources originate from within the organization. An effective user awareness of security countermeasures necessitates a careful implementation of security policies, education program and computer monitoring mechanisms, which generally entails a great extent of internal organizational knowledge. We contend that insider directors have a better access to information that is relevant to strengthen the user security education and training program. In a number of studies, top management support has proven to be important for the assimilation and effectiveness of information security management [Kankanhalli et al., 2003; Hsu et al., 2012]. Thus, we articulate that insider directors are more able to development an appropriate information security policy and demonstrate stronger effect on employees' attitude towards information security management. This would then reduce the possibilities of information security breaches in organizations. Second, the implementation of information security management requires regular review and continuous security management improvement in order to adapt varying environmental contingencies. For insider directors, they posit the advantages of receiving ongoing feedback within the organizational structure and initiating ongoing changes in organization's social structure. The chief enterprise risk officer from Visa corporation has commented that it is importance to the board members understand information security as "a business-process problem."[2] We consider the inside director would have a more comprehensive and insightful understanding of the organizational business process and practices than the independent directors. Third, as indicated by prior studies, senior management initiatives and the involvement in security programs and rewards for security-associated behavior can foster the creation of a security culture [Ranmachandran and Rao, 2006]. We consider that having a higher percentage of inside directors on the board can strengthen the strategic importance of management involvement in security management program within organization. Therefore, building on the arguments above, we hypothesize that

*Hypothesis 2: The proportion of independent directors is positively associated with the likelihood of information security breaches.*

*Age and Tenure*: In assessing the relation between board composition and firm performance,

2) http://online.wsj.com/news/articles/SB10001424052702304773104579266743230242538.

age and organizational tenure have been an interest of investigation for organizational theorists [Carter et al., 2003; Finkelstein and Hambrick, 1989; Johnson et al., 1993; Robinson and Dechant 1997). The main argument in this stream of literature is that the age and tenure is associated with the director's experience and cognitive capabilities in making effective decisions. TIAA-CREF [1997] states the board should be composed of "qualified individuals who reflect diversity of experience, gender, race and age" in its document about corporate governance. Similarly, the National Association of Corporate Directors suggests that firms need to consider director diversity when forming the board. In discussing age and tenure, average age of tenure as well as heterogeneity of those are the two aspects of particular interests to organizational researchers. Average age of board members is relevant with the cognitive ability in decision making. Scholars suggest that certain cognitive capabilities such as learning ability and memory seem to fade away with age and older managers have thought to hold a risk-averse attitude [Bantel and Jackson, 1989; Burke and Light, 1981]. By comparison, younger managers with a more recent education are open to innovation and knowledgeable of new technical know-how. With respect to organizational tenure, Pfeffer [1983] suggests that the similarity of educational and organizational experience usually serve a better common ground for mutual understanding and effective communication. The increasing group tenure offers the value to maintain stability and reduce group conflict during the decision-making process. In contrast, prior studies [Carter et al., 2003; Finkelstein and Hambrick, 1989; Johnson et al., 1993; Robinson and Dechant, 1997] have also emphasized the importance of the diversity of the board and as a representation of good corporate governance, such as better understanding of the environment, creativity and the effectiveness of problem solving.

In the context of information security, although younger directors might have a better technical know-how, the older the directors or the directors with a longer organizational tenure normally accumulated a wealth of experience and know-how, which allows them in a better position to advise managers when dealing with information security management issues faced by the organization. Similar to the argument presented earlier, the implementation of information security policies requires ongoing feedback and continuous improvement. More tenured and older directors are more likely to develop a better understanding of organization-specific security management issues and to commit in long-term improvement program. With this commitment, it would allow the development of a better information security policy and the demonstration of senior management support in the implementation of information security management in organizations. This consequently can mitigate the information security risks and reduce the potential information security breaches. Therefore, we believe that as the average age and/or average tenure of the directors increases, a firm can benefit from the increased knowledge of the board and reduce the likelihood of information security breaches.

As for heterogeneity of age and tenure, although we consider that on average having an older board is more beneficial to reduce the likelihood of information security breaches, we argue that given that the rapid technological chan-

ges and emerging security breaches, having a board with some young directors may strike the balance between the need for knowledge on innovative technologies from the younger directors and accumulated organizational or industry experiences from the older ones. Therefore, we argue that the heterogeneity of age of the board can reduce the likelihood of information security breaches.

By contrast, we believe that the heterogeneity of tenure may have a less favourable impact on a firm's security governance decision. Differing from age, Zenger and Lawrence [1989] consider that "tenure functions as an indicator of organizational experiences… of familiarity with the organizational language" (p.357). From this viewpoint, we contend that an effective implementation of security policies and user education program entails a great extent of internal organizational knowledge and strong management involvement. This is much easier in the situation when members of the board are more homogeneous because they share similar organizational and industry experiences. In other words, we argue that tenure heterogeneity may hinder the development of team cohesiveness and efficiency in decision-making, and thus would be positively associated the likelihood of information security breaches.

*Hypothesis 3a: The average age of the directors is negatively associated with the likelihood of information security breaches.*

*Hypothesis 3b: The heterogeneity of age of the directors is negatively associated with the likelihood of information security breaches.*

*Hypothesis 4a: The average tenure of the directors is negatively associated with the likelihood of information security breaches.*

*Hypothesis 4b: The heterogeneity tenure of the directors is positively associated with the likelihood of information security breaches.*

In addition to our hypotheses above, we explore the moderating effect of age and tenure of the directors on the role played by the size of the board and the independent directors on the likelihood of information security breaches.

# 4. Sample and Research Models

## 4.1 Data Collection

We used all the *S&P* 1500 firms from 1997 to 2009 as our sample. We chose this sample period because of the access limitation to the data about board of directors. Data about each firm's board of directors was collected from the *Risk Metrics* database. We then calculated the number of directors on the board and the number of independent directors[3] on the board in each firm for every year of the study period, as well as the age and tenure of each director. The calculation of the measures are discussed in Section 4.2.

Next, we searched the major media outlets for media reports on information security breaches as a measure of the consequence of in-

3) An independent director is a director who has not material relationships with the company, such as an executive or an employee. That is, an independent director can exercise independent judgment without other potential interferences due to the material relationship.

<Table 1> Variable Definitions

| Variable | Definition | Data Source |
|---|---|---|
| *Breach* | Equals 1 if the firm has information security breach announcement(s) at time *t*; 0 otherwise. | news articles |
| *CSize* | Size of the firm which equals the logarithm of the total assets at time *t*-1. | *Compustat* |
| *CAge* | Age of the firm which equals the logarithm of the age of the firm at time *t*-1. | *Compustat* |
| *M/B* | Market to book ratio of the firm which equals the market value of the firm divided by the common stockholders' equity at time *t*-1. | *Compustat* |
| *Ind* | Firms in the industry with two-digit SIC code of 73 | *Compustat* |
| *ITIntensity* | The ratio of annual IT capital per employee deflated by the average ratio of all industries at the three digit NACIS code level based on the statistics disclosed by the U.S. Bureau of Economic Analysis. | *Bureau of Economic Analysis* |
| *BSize* | Size of the board which equals the number of directors at time *t*-1. | *RiskMetrics* |
| *IBSizePer* | The average proportion of independent directors for each firm which is averaged in the sample period. | *RiskMetrics* |
| *avgAge* | Average age of the directors for each firm at time *t*-1. | *RiskMetrics* |
| *avgTenure* | Average tenure of the directors for each firm at time *t*-1. | *RiskMetrics* |
| *CVAge* | Heterogeneity of age; the coefficient of variation of age which equals the standard deviation divided by the mean at time *t*-1. | *RiskMetrics* |
| *CVTenure* | Heterogeneity of tenure; the coefficient of variation of tenure which equals the standard deviation divided by the mean at time *t*-1. | *RiskMetrics* |

formation security management at the firms of interest from 1997 to 2009. We searched *the Wall Street Journal, USA Today, the Washington Post*, and *the New York Times* using the *Factiva* database as well as the *CNet* and *ZDNet* websites. The search terms were: (1) security breach, (2) hacker, (3) cyber attack, (4) virus or worm, (5) computer break-in, (6) computer attack, (7) computer security, (8) network intrusion, (9) data theft, (10) identity theft, (11) phishing, (12) cyber fraud, and (13) denial of service. These search terms were similar to those used in prior studies [Campbell et al., 2003; Garg et al., 2003; Wang et al., 2012]. The incidents from the DataLossDB (http://datalossdb.org) were used to further verify our search results.[4] We then cross-checked the derived information security breach reports with the sample of *S&P 1500* firms. If a firm in our sample figured in a security breach report, we set the value of the variable Breach at 1, and zero otherwise (see <Table 1> for variable definitions).[5] The resulting sample size was 32,479 executive-year-event observations from 63 industries. As shown in <Table 2>, though six industries (two-digit SIC code 28, 35, 36, 49, 60, and 73) dominate more than 5% of the overall size, our industry distribution is indistinguishable at the firm level as the Compustat universe (the *p*-value for the Kolmogorov-Smirnov test is almost 1.00).

4) See http://online.wsj.com/news/articles/SB110869-427983158632?mod=_newsreel_4 for an example of the news article.

5) It is possible that a firm may have multiple reported security breaches in a certain year. For the rest of the paper, we only present the case when only the first reported security breach is included. Our results are similar when we delete all the multiple security breaches for a single firm in a certain year.

<Table 2> Industry BreakdownTable 2: Industry Breakdown

| Name of the Industry | % in Our Sample | % in Compu-stat | Name of the Industry | % in Our Sample | % in Compu-stat |
|---|---|---|---|---|---|
| metal mining | 0.82% | 2.81% | communications | 3.00% | 3.34% |
| coal mining | 0.16% | 0.23% | electric, gas, services | 5.34% | 2.62% |
| oil extraction | 3.13% | 5.00% | wholesale durable | 1.94% | 2.17% |
| quarrying minerals | 0.16% | 0.29% | wholesale non-durable | 1.15% | 1.31% |
| building construction | 0.56% | 0.54% | building materials, hardware | 0.30% | 0.22% |
| heavy construction | 0.30% | 0.25% | general merchandise stores | 1.05% | 0.61% |
| special trade contractors | 0.16% | 0.27% | food stores | 0.63% | 0.63% |
| food products | 2.14% | 2.11% | auto dealers and gas stations | 0.43% | 0.29% |
| tobacco products | 0.16% | 0.10% | apparel and accessory stores | 1.52% | 0.55% |
| textile mill products | 0.63% | 0.63% | home furniture, furnishings | 0.59% | 0.45% |
| apparel and others | 0.86% | 0.91% | eating and drinking places | 1.55% | 1.27% |
| wood products | 0.49% | 0.50% | miscellaneous retail | 1.78% | 1.56% |
| furniture and fixtures | 0.40% | 0.42% | depository institutions | 6.99% | 6.66% |
| paper products | 1.38% | 0.81% | non-depository credit institutions | 0.92% | 1.72% |
| printing, publishing | 1.32% | 1.20% | security and commodity brokers | 1.71% | 1.07% |
| chemicals products | 6.23% | 5.23% | insurance carriers | 4.05% | 1.73% |
| petroleum refining | 0.86% | 0.49% | insurance agents and service | 0.46% | 0.39% |
| rubber | 0.82% | 1.00% | real estate | 0.13% | 1.51% |
| leather products | 0.26% | 0.20% | investment offices | 2.83% | 9.70% |
| stone, glass products | 0.56% | 0.62% | hotels, rooming houses, others | 0.30% | 0.52% |
| primary metal | 1.75% | 1.16% | personal services | 0.30% | 0.26% |
| fabricated metal | 1.09% | 1.41% | business services | 9.92% | 9.41% |
| computer equipment | 5.74% | 4.54% | automotive repair, services | 0.16% | 0.22% |
| electronic and others | 6.76% | 5.27% | motion pictures | 0.40% | 0.80% |
| transportation equipment | 2.34% | 1.63% | recreation services | 0.92% | 0.99% |
| measuring instruments | 4.88% | 4.23% | health services | 2.08% | 1.51% |
| mis. manuf. industries | 0.82% | 0.98% | educational services | 0.40% | 0.29% |
| railroad transportation | 0.33% | 0.21% | social services | 0.10% | 0.12% |
| transit and transportation | 0.13% | 0.07% | research, management, services | 1.38% | 1.52% |
| warehousing | 0.63% | 0.62% | nonclassifiable establishments | 0.36% | 1.25% |
| water transportation | 0.26% | 0.41% | | | |
| transportation by air | 0.69% | 0.63% | | | |
| transportation services | 0.46% | 0.35% | | | |

## 4.2 Measures and Research Models

As identified above, our research objective is to investigate whether the board structure is associated with the possibility of breach announcements (*Breach*). To operationalize this, we calculated the number of directors (*BSize*) and the percentage of independent directors (*IBSize*) in

a firm for each year from 1997 to 2009. For the measure of age and tenure, we calculated the average age of the directors and the average tenure (in days) in the firm for each year. Then we used the commonly adopted measure "coefficient of variation" to capture the heterogeneity of age and tenure [Williams and O'Reilly, 1998] which equals the standard deviation divided by the mean of age and tenure (*CVAge* and *CVTenure*) also for each year. Furthermore, similar to prior literature [Cavusoglu et al., 2004; Wang et al., 2012], we controlled for firm size (*CSize*, logarithm of total assets (in millions) of the firm at the beginning of the year) and industry (*Ind*) for our analysis. For industry, we consider the firms in the industry with two-digit SIC code of 73 since (1) SIC code 73 has a majority of firms engaging in information technology and communication related businesses. For example, on-line advertisement, search engine, data file services, internet security services, and etc. These firms' revenue generating processes can be severely damaged by information security breaches and are more vulnerable to security incidents, and (2) this is the industry with the largest number of observations in our sample. As a robustness test, we consider a second measure of the potential industry differences. This second measure is IT intensity (*ITIntensity*). Following prior literature (e.g., [Kwon et al., 2013]), we calculate the ratio of annual IT capital per employee deflated by the average ratio of all industries at the three digit NACIS code level based on the statistics disclosed by the U.S. Bureau of Economic Analysis. We also controlled for the age of the firm (*CAge*) and the market-to-book ratio (*M/B*) which equals the market value of the firm divided by the common stock holders' equity at the beginning of the year. The age of the firm and the market-to-book ratio reflect a firm's inherent uncertainty which could affect the likelihood of information security breaches. Last, we control for the year effect in our model.

The descriptive statistics and the correlation of the variables are given in <Table 3> and <Table 4>. As given in <Table 3>, there are fewer observations for the board structure measures

<Table 3> Descriptive Statistics

| Variable | N | Mean | Std Dev | Quartiles | | |
|---|---|---|---|---|---|---|
| | | | | Q1 | Q2 | Q3 |
| *Breach* | 32,479 | 0.01 | 0.095 | 0.00 | 0.00 | 0.00 |
| *CSize* | 32,454 | 3.13 | 0.770 | 2.58 | 3.05 | 3.62 |
| *CAge* | 32,478 | 1.22 | 0.315 | 1.00 | 1.20 | 1.46 |
| *Ind* | 32,479 | 0.17 | 0.377 | 0.00 | 0.00 | 0.00 |
| *ITIntensity* | 32,439 | 2.29 | 2.453 | 0.410 | 1.601 | 2.984 |
| *M/B* | 32,454 | 3.53 | 41.118 | 1.49 | 2.32 | 3.86 |
| *BSize* | 21,160 | 9.20 | 2.814 | 7.00 | 9.00 | 11.00 |
| *IBSizePer* | 19,517 | 0.17 | 0.248 | 0.06 | 0.08 | 0.11 |
| *avgAge* | 27,335 | 52.30 | 6.170 | 48.25 | 52.00 | 56.00 |
| *avgTenure* | 27,335 | 12.35 | 9.324 | 5.00 | 10.00 | 17.40 |
| *CVAge* | 27,335 | 0.09 | 0.082 | 0.00 | 0.09 | 0.15 |
| *CVTenure* | 26,902 | 0.45 | 0.428 | 0.00 | 0.41 | 0.74 |

<Table 4> Pearson Correlation

| | *Breach* | *CSize* | *CAge* | *Ind* | *IT-Intensity* | *M/B* | *BSize* | *IB-SizePer* | *avgAge* | *avg-Tenure* | *CVAge* | *CV-Tenure* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Breach* | 1.00 | | | | | | | | | | | |
| *CSize* | 0.14*** | 1.00 | | | | | | | | | | |
| *CAge* | 0.03*** | 0.39*** | 1.00 | | | | | | | | | |
| *Ind* | -0.01** | -0.21*** | -0.19*** | 1.00 | | | | | | | | |
| *ITIntensity* | 0.04*** | 0.15*** | -0.125*** | 0.116** | 1.00 | | | | | | | |
| *M/B* | -0.00 | -0.01* | 0.00 | -0.00 | -0.01** | 1.00 | | | | | | |
| *BSize* | 0.07*** | 0.60*** | 0.37*** | -0.24*** | 0.15*** | -0.01 | 1.00 | | | | | |
| *IBSizePer* | 0.08*** | -0.01 | 0.01 | 0.03*** | 0.02*** | 0.00 | -0.09*** | 1.00 | | | | |
| *avgAge* | 0.01* | 0.24*** | 0.34*** | -0.17*** | -0.08*** | -0.01 | 0.22*** | -0.08*** | 1.00 | | | |
| *avgTenure* | 0.01** | 0.21*** | 0.26*** | -0.11*** | -0.07*** | 0.01 | 0.19*** | -0.18*** | 0.46*** | 1.00 | | |
| *CVAge* | -0.01 | -0.14*** | -0.17*** | 0.02*** | 0.01* | 0.00 | -0.12*** | 0.05*** | -0.12*** | -0.02*** | 1.00 | |
| *CVTenure* | 0.02*** | -0.07*** | -0.10*** | 0.03*** | 0.07*** | -0.00 | -0.05*** | 0.14*** | -0.16*** | -0.25*** | 0.48*** | 1.00 |

***significant at 1% **significant at 5% *significant at 10%.

due to missing values in the database. In <Table 4>, note that the size of the firm (*CSize*) is positively and significantly correlated with board size (*BSize*) (0.602, $p < 0.01$). We acknowledge that such a correlation could be problematic if these variables are included in the same model. To further investigate this issue, we first regress board size on firm size then use the residuals from the regression to replace board size. Our results remain similar. In addition, we checked the VIF values for the main variables in our regression models later. The lowest value is 1.004 and the highest value is 3.442, which is for board size. The VIF value reduces to below 3 after we replace the board size with the residuals and our results remain similar.

Based on our measures, we use Equation (1), Equation (2) and Equation (3) below to test our Hypotheses. Equation (1) focuses on age of the directors while Equation (2) considers tenure of the directors. Equation (3) takes into account both age and tenure in the same model. The dependent variable for these equations is *Breach* for firm *i* at time *t*. In these two equations, the independent variables are those defined earlier and are for firm i at time *t*-1, where the $\beta_j$ are the coefficients and $\varepsilon$ is the residual terms. We estimate the coefficients using the logistic regression model. Logistic regressions have been widely used in risk management contexts when the dependent variable is binary, such as operational risks, and information security risks (e.g., [Wang and Hsu, 2013; Hsu and Wang, 2014; Kwon et al., 2013]). Since we consider the likelihood of the occurrence of reported information security breaches, which is a binary variable (i.e., with reported breach or without reported breach), we also use logistic regression models.

$$\begin{aligned} Breach_{it} = {} & \beta_0+\beta_1 CSize_{it-1}+\beta_2 CAge_{it-1}+\beta_3 Ind_{it-1} \\ & +\beta_4 M/B_{it-1}+\beta_5 BSize_{it-1}+\beta_6 IBSizePer_{it-1} \\ & +\beta_7 avgAge_{it-1}+\beta_8 CVAge_{it-1}+\beta_9 BSize_{it-1} \\ & \times avgAge_{it-1}+\beta_{10} BSize_{it-1}\times CVAge_{it-1} \\ & +\beta_{11} IBSizePer_{it-1}\times avgAge_{it-1} \\ & +\beta_{11} IBSizePer_{it-1} \times CVAge_{it-1} + \Sigma Year \\ & + \varepsilon_{1it} \end{aligned} \quad (1)$$

$$Breach_{it} = \beta_0+\beta_1 CSize_{it-1}+\beta_2 CAge_{it-1}+\beta_3 Ind_{it-1} \quad (2)$$
$$+\beta_4 M/B_{it-1}+\beta_5 BSize_{it-1}+\beta_6 IBSizePer_{it-1}$$
$$+\beta_7 avgTenure_{it-1}+\beta_8 CVTenure_{it-1}$$
$$+\beta_9 BSize_{it-1}\times avgTenure_{it-1}+\beta_{10} BSize_{it-1}$$
$$\times CVTenure_{it-1}+\beta_{11} IBSizePer_{it-1}$$
$$\times avgTenure_{it-1}+\beta_{11} IBSizePer_{it-1}$$
$$\times CVTenure_{it-1}+\Sigma Year+\varepsilon_{2it}$$

$$Breach_{it} = \beta_0+\beta_1 CSize_{it-1}+\beta_2 CAge_{it-1}+\beta_3 Ind_{it-1} \quad (3)$$
$$+\beta_4 M/B_{it-1}+\beta_5 BSize_{it-1}+\beta_6 IBSizePer_{it-1}$$
$$+\beta_7 avgAge_{it-1}+\beta_8 CVAge_{it-1}$$
$$+\beta_9 avgTenure_{it-1}+\beta_{10} CVTenure_{it-1}$$
$$+\beta_{11} BSize_{it-1}\times avgTenure_{it-1}+\beta_{12} BSize_{it-1}$$
$$\times CVTenure_{it-1}+\beta_{13} BSizePer_{it-1}$$
$$\times avgTenure_{it-1}+\beta_{14} IBSizePer_{it-1}$$
$$\times CVTenure_{it-1}+\Sigma Year+\varepsilon_{3it}$$

# 5. Analysis and Results

## 5.1 Main Empirical Results

The results are given in <Table 5>. For Equation (1) (the second column in <Table 5>), the significant negative coefficient (-0.702 and -0.782, $p < 0.01$) for the variable *BSize* supports our Hypothesis 1a that security breaches are less likely to occur when the board is larger. As we indicated earlier, there are contrasting arguments considering the merits of having a larger board size. Our result shows that having a larger board is more preferable from the perspective of information security management. Our results offer the empirical evidence that when the board size grows, the benefit of accessing to a diverse knowledge is crucial from the standpoint of decision-making quality. This finding extends to the previous argument that a larger board can bring more knowledge and recourses in designing and articulating a more effectiveness information security governance framework.

Next, our analysis of board characteristics indicates that the percentage of independent directors in the board is positively in Equation (2) (1.455 and 1.376, $p < 0.05$ and $p < 0.10$) associated with the possibility of security breaches. This supports our hypotheses and previous arguments about the importance of internal directors in contributing to organizational knowledge for better information security governance. Prior literature has shown that though outside directors could provide their experience and outside resources to the firm [Ellstrand et al., 2002], they might not have enough time and internal knowledge to make informed decisions especially when the decision requires knowledge of the firm's capabilities [Baysinger and Hoskisson, 1990; Lorsch and Maclver, 1989]. In our information security context, in order for managers to better manage information security risks and implement effective information technology controls, it is inevitable to understand how a firm's strategy interacts with its environment and its capabilities [Applegate et al., 2009]. Accordingly, though the number of independent directors could enhance the monitoring function of the board and provide external resources to the firm, the board needs to have more internal knowledge of value and risk when facing information security challenges. Therefore, the internal knowledge function of the board is more important than the monitoring function in the security context.

Furthermore, we find that the older the directors, the smaller will be the possibility of security breaches (the coefficient of *avgAge* is significantly negative in all models). Similarly, the

average tenure is negatively associated with the possibility of security breaches in Equation (2) (the coefficient of *avgTenure* is -0.065 and -0.074, $p < 0.10$). The results support hypothesis 3a and 4a that the older the directors are or the longer the tenure the directors means that these directors have accumulated a wealth of experience and know-how, which allows them in a better position to advise managers when dealing with information security management issues faced by the organization. Focusing on the issue of board heterogeneity, the results in <Table 5> also support Hypothesis 3b (the coefficient of *CVAge* is significantly negative in most of the models) and Hypothesis 4b (the coefficient of *CVTenure* is significantly positive in all cases). The results suggest that though board diversity in terms of age could be an important aspect in corporate governance and reduce the possibility of information security breaches. However, the diversity on tenure could be a communication barrier among the directors [Zenger and Lawrence, 1989] and affect the decision making process which could oppositely make the board less effective and in turn increase the possibility of breaches. Furthermore, studies have shown that the heterogeneity in directors' ability to give advice can affect firm value and major firm decisions which cannot be explained by board size [Knyazeva et al., 2009]. In our security context, our finding suggests that age and tenure plays an important role when facing security risks. As we point out earlier, the development of a security management program including the security policy, management committee, team structure (e.g., CISO or security officers), risk management process and employee education to preserve the confidentiality, integrity and availability of information in organizations. All these tasks require an enterprise-wide implementation and demand the talent and skills of management to executive them well. Furthermore, given the emerging nature of information security management, the depth of managerial experiences from the board becomes significantly invaluable to the top management team.

## 5.2 Moderating Effects

It is also possible that age and tenure may moderate the effect of board size and the percentage of independent director on the likelihood of information security incidents. The results in <Table 5> suggest that the average age and average tenure positively affect the association between board size and the possibility of information security breach (the coefficients of *BSize×avgAge* and *BSize×avgTenure* are significantly positive in most of the cases). Similarly, the heterogeneity of age (*cvAge*) also positively affects the association between board size (*BSize*) and possibility of security breach. Differently, the heterogeneity of tenure (*cvTenure*) negatively affects the relation between board size (*Bsize*) and the possibility of security breach. In summary, as the average age, average tenure, or the heterogeneity of age increases, the association between board size and the likelihood of information security breaches becomes less negative. On the contrary, as the heterogeneity of tenure increases, the relation between board size and the likelihood of information security breaches is more negative. Interestingly, our findings do not show any moderating effect of age and tenure on the percentage of independent directors on the likelihood of security breaches.

<Table 5> Empirical Results

| Variable | Equation (1) | Equation (1) | Equation (2) | Equation (2) | Equation (3) Without Interaction Terms | Equation (3) | Equation (3) Without Interaction Terms | Equation (3) |
|---|---|---|---|---|---|---|---|---|
| Intercept | -1.304 | -0.309 | -11.460*** | -10.926*** | -10.228*** | -3.261 | -9.548*** | -2.222 |
| *CSize* | 1.655*** | 1.576*** | 1.620*** | 1.507*** | 1.617*** | 1.604*** | 1.511*** | 1.502*** |
| *CAge* | -0.468 | -0.62 | -0.280 | -0.052 | -0.288 | -0.309 | -0.117 | -0.070 |
| *Ind* | 0.650*** | | 0.673*** | | 0.637*** | 0.581** | | |
| *ITIntensity* | | 0.109*** | | 0.125*** | | | 0.121*** | 0.127*** |
| *M/B* | -0.002 | -0.001 | -0.002 | -0.001 | -0.002 | -0.002 | -0.001 | -0.002 |
| *BSize* | -0.702*** | -0.782*** | 0.045 | -0.014 | 0.055 | -0.474 | 0.033 | -0.541 |
| *IBSizePer* | 0.247 | 0.238 | 1.455** | 1.376* | 1.480** | -1.501 | 1.393** | -1.765 |
| *avgAge* | -0.179*** | -0.192*** | | | -0.025* | -0.153** | -0.034** | -0.166** |
| *CVAge* | -9.470* | -10.531** | | | -1.490 | -20.619*** | -1.727 | -21.011*** |
| *avgTenure* | | | -0.065* | -0.074* | 0.008 | -0.017 | 0.017 | -0.022 |
| *CVTenure* | | | 1.734** | 1.498* | 0.533** | 3.430*** | 0.517** | 3.272*** |
| *BSize×avgAge* | 0.013*** | 0.014*** | | | | 0.010* | | 0.010* |
| *BSize×CVAge* | 0.851** | 0.935** | | | | 1.650*** | | 1.649*** |
| *BSize×avgTenure* | | | 0.006** | 0.007** | | 0.002 | | 0.003 |
| *BSize×CVTenure* | | | -0.142** | -0.122* | | -0.281*** | | -0.264*** |
| *IBSizePer×avgAge* | 0.026 | 0.869 | | | | 0.057 | | 0.060 |
| *IBSizePer×CVAge* | 0.747 | 0.022 | | | | 3.195 | | 3.688 |
| *IBSizePer×avgTenure* | | | -0.002 | -0.003 | | -0.011 | | -0.014 |
| *IBSizePer×CVTenure* | | | 0.433 | 0.408 | | 0.111 | | 0.030 |
| Year Effect | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| *Model Chi-Square* | 530.28 | 531.72 | 503.87 | 507.00 | 495.48 | 519.40 | 499.08 | 524.41 |
| *Pseudo* $R^2$ | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 |
| *N* | 17,386 | 17,376 | 17,106 | 17,096 | 17,106 | 17,106 | 17,096 | 17,096 |

***significant at 1% **significant at 5% *significant at 10%

## 5.3 Robustness Tests

To further validate our results, we first re-perform our analyses based on different age and tenure groups. Given that the two industry effect measures result in similar main results, we only present Ind in the following robustness tests. The results are given in <Table 6>. First, note that for the smallest heterogeneity of age and tenure group, we do not have any firms with reported breaches. Accordingly, we are not able to estimate the coefficients. Second, the results are largely similar to those in our main analyses except for the groups for tenure. We further examine the data of the tenure group. The data shows that the majority of the average tenure value for the smallest tenure group is 0 and 1 with a range between 0 and 4. For the largest tenure group, the value can be from 20 to 55. When we only look at the extremes, these extreme values provide insignificant or different results from our main analyses. The results also suggest a wide range of tenure in our observations.

<Table 6> Empirical Results for Different Age and Tenure Group

| *Variable* | *avgAge* | | *CVAge* | | *avgTenure* | | *CVTenure* | |
|---|---|---|---|---|---|---|---|---|
| | *Largest 20%* | *Smallest 20%* | *Largest 20%* | *Smallest 20%* | *Largest 20%* | *Smallest 20%* | *Largest 20%* | *Smallest 20%* |
| *Intercept* | -21.580* | 7.897 | 96.266*** | | -16.102*** | -33.105*** | -11.261** | |
| *CSize* | 2.103*** | 0.780* | 3.100*** | | 1.985*** | 0.386 | 0.699** | |
| *CAge* | -3.054*** | -1.141 | 0.936 | | -0.189 | -2.076 | 1.961** | |
| *Ind* | 1.366** | -0.168 | 2.271* | | 0.912* | 1.072 | 1.644*** | |
| *M/B* | -0.007 | -0.045 | 0.028 | | -0.004 | 0.046 | 0.010 | |
| *BSize* | 1.132 | -0.596 | -5.098** | | 0.470 | 1.199*** | 0.183 | |
| *IBSizePer* | -3.839 | 6.700 | -8.379 | | 1.587 | 19.326** | -1.347 | |
| *avgAge* | 0.155 | -0.395 | -2.475*** | | | | | |
| *CVAge* | -58.341*** | -2.102 | -19.615 | | | | | |
| *avgTenure* | | | | | 0.157 | 2.485 | 0.037 | |
| *CVTenure* | | | | | 0.982 | 2.911 | -1.153 | |
| *BSize×avgAge* | -0.018 | 0.013 | 0.136*** | | | | | |
| *BSize×CVAge* | 4.302*** | 0.681 | -3.724 | | | | | |
| *BSize×avgTenure* | | | | | -0.012 | -0.275* | -0.000 | |
| *BSize×CVTenure* | | | | | -0.026 | -0.336 | -0.247 | |
| *IBSizePer×avgAge* | 0.144 | -0.028 | 0.350 | | | | | |
| *IBSizePer×CVAge* | 13.123 | 2.566 | -32.544 | | | | | |
| *IBSizePer×avgTenure* | | | | | -0.114 | 0.186 | -0.184* | |
| *IBSizePer×CVTenure* | | | | | -2.094 | 1.631 | 6.162** | |
| *Year Effect* | Yes | Yes | Yes | | Yes | Yes | Yes | |
| *Model Chi-Square* | 175.60 | 69.56 | 253.90 | | 216.96 | 85.81 | 90.16 | |
| *Pseudo $R^2$* | 0.05 | 0.02 | 0.08 | | 0.05 | 0.03 | 0.03 | |
| *N* | 3,775 | 2,984 | 3,237 | | 4,163 | 2,614 | 3,134 | |

*** significant at 1% ** significant at 5% * significant at 10%, note that we do not have enough observations for the smallest 20% of CVAge and CVTeure.

Second, in <Table 7>, we further consider the IT background and IT experience of the directors in our sample. Due to data limitation, we are only able to gather the data from Bloomberg database for 2008 and 2009 with many missing values. The total number of observations (executive-year-event observations) is 823 for our analyses. The results need to be interpreted with caution given the limited data access. As given in <Table 7>, the coefficient for the percentage of independent director is still positive. However, IT background and IT experience do not affect the possibility of security breaches. Last, in our main analyses, it is performed based on executive-year-event data. We further control for the firm effect and the executive effect. Due to the larger number of zeros for the firm and executive dummies, the model becomes insignificant (the $p$ value of the F-test is larger than 0.1).

<Table 7> Empirical Results for IT Background and IT Experience

| Variable | |
|---|---|
| *Intercept* | -13.459*** |
| *CSize* | 1.896*** |
| *CAge* | -2.991*** |
| *Ind* | 0.217 |
| *M/B* | -0.009 |
| *BSize* | -0.049 |
| *IBSizePer* | 8.746** |
| *ITBackground* | -63.448 |
| *ITExperience* | 3.024 |
| *BSize×ITBackground* | 15.587 |
| *BSize×ITExperience* | 0.044 |
| *IBSizePer×ITBackground* | -152.700 |
| *IBSizePer×ITExperience* | -3.663 |
| *Year Effect* | Yes |
| *Model Chi-Square* | 61.85 |
| *Pseudo* $R^2$ | 0.07 |
| *N* | 823 |

***significant at 1% **significant at 5% *significant at 10%

Last, we control for firm specific fixed effects and our results remain similar. In addition, we also explored whether security breaches would be associated with future changes in the board structure. However, due to the fact that board composition does not change frequently, we did not observe any significant association.

## 6. Implication and Conclusions

This study focuses on the guidance role played by a firm's board of directors and investigates how the board's structure impacts the effectiveness of security management in terms of preventing or reacting to security breaches. The findings shown in this study has several theoretical and practical implications. First, our exploratory results indicate that the board composition plays a role in information security management. We see these findings add theoretical value to the existing organizational approach to information security management research. As indicated earlier, the involvement of management and end-user have been examined and studied in relation to information security program and its effectiveness. Emphasis on the board composition is emerging, but to our best of knowledge, no scholarly assessment has been performed in the context of information security governance. Our results show that the demographic characteristics of the board have a significant impact on the possibility of information security breaches in the firms. In addition to demographic characteristics, we consider other possible research areas that might worth exploring further. For instance, what is the moderating impact of board incentive on the effec-

tiveness of information security governance? Will different compensating and rewarding mechanism play a role in the board's decision in the context of information security governance? Second, we consider our work contributing to the existing corporate governance literature. For historical reason, the scope of corporate governance has focused on the analysis between the board and firm performance. Traditionally, the elements of information security governance and control have been implicitly discussed within the board concept of corporate governance. Nonetheless, we believe that with the increasing demand of regulatory compliance and the role of technology for internal control, the board is assigned with an additional responsibility to ensure that managers are acting in a responsible matter to safeguard the critical information assets in the organizations. Our work here might add a fresh perspective in the theorization of board structure for modern organizations. One valuable implication is to contribute the debate on the proportion of insider directors and independent directors serving on the board, and its correlation on firm performance. Agency scholars believe that board dependence, i.e., the dominance of insider director, weakens the monitoring function and is negatively associated with firm performance [Core et al., 1999; Daily and Dalton, 1994]. Our result argues that when considering information security governance, one might need to waive the benefit of impartiality of outside director for the value of insider directors who hold the in-depth and firm-specific knowledge about risks faced by the firms. Thus, identifying the mechanisms and variables in addressing this balance warrants further research attention. Furthermore, we consider that our findings have theoretical implications towards the information security culture and risk management. This study suggests that the older directors are associated with a smaller possibility of information security breaches. This implies that these directors are relatively knowledgeable and experienced in understanding organization-specific security culture and risks. We believe this understanding would facilitate the managers to develop appropriate information security culture program and risk management approach.

From the practical perspective, the directors need to consider both the value of IT and the potential risk and consequences that might follow. This also has practical implications on the appropriate training and education offered to the directors. Drawing from our study, we argue that it might become necessary to offer information security risk management education to the board of directors. Such education is important to facilitate the directors in articulating corporate strategy for information security governance and risk management. For example, the case of computer malfunction in Tokyo Stock Exchange in 2005 led to the loss over 40 billion Yen, which also resulted in the resignation of exchange CEO and two other senior executives for the inadequate IT planning, governance and crisis management at the senior management and board level. Another example is the resignation of the board member and senior management at HP in 2006 because of the violation of privacy regulation. These two examples highlight the significance of board oversight and information security awareness at board level for an effective information security program within an organization. A sound education and awareness program for the board of

directors can improve the quality of decision-making and board oversight, hence, mitigate the risk of information security breaches in a company.

Furthermore, though our findings do not suggest an optimal board structure and composition, we point out the elements that need to be paid attention to when forming the board or given the current board structure and composition a firm has. Since generally larger firms have larger board size, the quality of decision becomes an issue when managing security risks. Also, firms need to focus more on the communication within different age/tenure groups and how to better utilize outside resources independent directors can have. As shown in the survey of PwC 2012 Global State of Information Security Survey,[6] the findings highlight the imperative of communication and collaboration at the board level in articulating a clear information security vision and strategy. Last, though external resources are valuable to the firm, it needs to balance the industry-wide as well as the enterprise-wide knowledge when looking for independent directors especially when the firm faces larger uncertainty in terms of information security. Our suggestion is that considering the knowledge specificity of information security management, the search strategy for independent director shall focus the domain of expertise rather than the number of directors. In doing so, the quality of board oversight on information security management is likely to be more effective.

We also recognize the limitations of this study, some of which offer opportunities for future research. First, although the use of secondary data has been a common practice in studying board composition, we suggest that research can further develop to collect board information and decision making process through survey or interview methods. Our exploratory results have highlighted the relevance of board composition and the likelihood of information security breaches in organizations. Case study or empirical survey results could help to offer insightful understanding into the group dynamics of the board and information security governance. In this case, the effectiveness of information security management may be better measured or proxied. Second, this research study only examined a common set of variables in board structure. This research provides a starting point for similar future studies in this area. For future research, we believe that other variables in corporate governance literature such as CEO duality or product market competition can contribute our knowledge about the impact of board structure on the effectiveness of information security management. Third, this study draws on the perspective of organizational demography and group dynamics in decision-making process to analyze the impact of board on information security governance. Another interesting study can examine the other conditions that may have moderating effects on the board decision-making process. For example, it is possible that the content and quality of information security policy might influence the decision-making quality of the board of directors. Fourth, we share the same limitation with prior studies that we are not able to obtain information regarding firm specific IT and/or information security related risk factors which may also affect the likelihood

6) http://www.pwc.com/jg/en/media-article/2012-global-state-of-information-security-survey.jhtml.

of information security breaches. If the data is available through surveys, future research can examine IT investment or information security policy's moderating effects on a firm's corporate governance on the effectiveness of information security risks. In addition, we share similar limitation with prior studies that we do not have access to firm level IT intensity data, which can be a major factor that affects the possibility of information security breaches. Last, though we have done our best to control for the size effect on information security breaches, it is arguable that the firms with reported security breaches are biased. However, given that we have obtained all the possible data points regarding board structure, we believe the effect is minimal.

In summary, this research argues for the strategic imperative of board composition on the effectiveness of information security management in organizations. Drawing on the organizational demography research, we conduct an exploratory empirical investigation to support the relevance of the above argument. Given the dynamics of information security management and the diversity of board structure, more theoretical and empirical enquiries can strengthen our understanding on this area. And we hope that our work here offers the starting point to inspire further research in this area.

## 〈References〉


[1] Applegate, L., Austin, R., and McFarlan, F.W., *Corporate Information Strategy and Management : Text and Cases*, (8th ed.). Boston: McGraw-Hill Irwin, 2009.

[2] Backhouse, J., Hsu, C.W., and Silva, L., "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly*, Vol. 30, 2006, pp. 413-438.

[3] Bantel, K. and Jackson, S., "Top Management and Innovations in Banking: Does the Composition of the Top Team Make a Difference," *Strategic Management Journal*, Vol. 10, 1989, pp. 107-124.

[4] Baskerville, R.L., *Strategic Information Security Risk Management*, 2008.

[5] Baysigner, B.D. and Butler, H.N., "Corporate Governance and the Board of Directors: Performance Effects of Changes in Board Composition," *Journal of Law, Economics and Organization*, Vol. 1, 1985, pp. 101-124.

[6] Baysinger, B. and Hoskisson, R.E., "The Composition of Boards of Directors and Strategic Control: Effects on Corporate Strategy," *The Academy of Management Review*, Vol. 15, No. 1, 1990, pp. 72-87.

[7] Beasley, M.S., "An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud," *The Accounting Review*, Vol. 71, No. 4, 1996, pp. 443-465.

[8] Burke, D. and Light, L., "Memory and Aging: The Role of Retrieval Processes," *Psychological Bulletin*, Vol. 90, 1981, pp. 513-546.

[9] Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L., "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11, 2003, pp. 431-448.

[10] Carr, N.G., "IT Doesn't Matter," *Harvard Business Review*, 2003, pp. 41-49.

[11] Carter, D.A., Simkins, B.J., and Simpson, W.G., "Corporate Governance, Board Diversity, and Firm Value," *The Financial Review*, Vol. 38, 2003, pp. 33-53.

[12] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, Vol. 9, 2004, pp. 70-104.

[13] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research*, Vol. 16, 2005, pp. 28-46.

[14] Chai, S., Kim, M., and Rao, H., "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior," *Decision Support Systems*, Vol. 50, 2011, pp. 651-661.

[15] Chang, S.E., and Ho, C.B., "Organizational Factors to the Effectiveness of Implementing Information Security Management," *Industrial Management and Data Systems*, Vol. 106, No. 3, 2006, pp. 345-361.

[16] Ciborra, C., "Imbrication of Representations: Risk and Digital Technologies," *Journal of Management Studies*, Vol. 43, 2006, pp. 1339-1356.

[17] Core, J.E., Holthausen, R.W., and Larcker, D.F., "Corporate Governance, "Chief Executive Office Compensation, and Firm Performance," *Journal of Financial Economics*, Vol. 51, 1999, pp. 371-406.

[18] D'Arcy, J., Hovav, A., and Galletta, D., "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, Vol. 20, 2009, pp. 79-98.

[19] Daily, C.M. and Dalton, D.R., "Bankruptcy and Corporate Governance: The Impact of Board Composition and Structure," *The Academy of Management Journal*, Vol. 37, No. 6, 1994, pp. 1603-1617.

[20] Deloitte, "2009 TMT Global Security Survey," 2009.

[21] Dhillon, G. and Torkzadeh, G., "Value-Focused Assessment of Information System Security in Organizations," *Information Systems Journal*, Vol. 16, 2006, pp. 293-314.

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

[23] Ellstrand, A.E., Tihanyi, L., and Johnson, J.L., "Board Structure and International Political Risk," *The Academy of Management Journal*, Vol. 45, 2002, pp. 769-777.

[24] Finkelstein, S. and Hambrick, D.C., "Chief Executive Compensation: A Study of the Intersection of Markets and Political Processes," *Strategic Management Journal*, Vol. 10, 1989, pp. 121-134.

[25] Forker, J.J., "Corporate Governance and Disclosure Quality," *Accounting and Business Research,* Vol. 22, No. 86, 1992, pp. 111-124.

[26] Garg, A., Curtis, J., and Halper, H., "Quantifing the Financial Impact of IT Security Breaches," *Information Management and Computer Security*, Vol. 11, 2003, pp. 74-83.

[27] Goel, S. and Shawky, H., "Estimating the Market Impact of Security Breach Annoucements on Firm Values," *Information and Management*, 46, 2009, pp. 404-410.

[28] Goodstein, J., Gautam, K., and Boeker, W.,

"The Effects of Board Size and Diversity on Strategic Change," *Strategic Management Journal*, Vol. 15, 1994, pp. 241-250.

[29] Gordon, L.A. and Loeb, M.P., "The Economics of Information Security Investment," *ACM Transactions on Information and System Security,* Vol. 5, No. 4, 2002, pp. 438-457.

[30] Gordon, L.A. and Loeb, M.P., "Budgeting Process for Information Security Expenditures," *Communications of the ACM*, Vol. 49, No. 1, 2006, pp. 121-125.

[31] Harrison, J.R., "The Strategic Use of Corporate Board Committees," *California Management Review*, Vol. 30, 1987, pp. 109-125.

[32] Herath, T. and Rao, H.R., "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, Vol. 47, 2009, pp. 154-165.

[33] Hsu, C. and Wang, T., Composition of the Top Management Team and Information Security Breaches. In Maria Manuela Cruz-Cunha (Ed.), Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, Pennsylvania: IGI Global, 2014.

[34] Hsu, C.W., "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems*, Vol. 18, 2009, pp. 140-150.

[35] Jensen, M.C. and Meckling, W.H., "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *Journal of Financial Economics*, Vol. 3, 1976, pp. 305-360.

[36] Jensen, M.C., "The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems," *Journal of Finance*, Vol. 48, 1993, pp. 831-880.

[37] Johnson, R.A., Hoskisson, R.E., and Hitt, M.A., "Board of Director Involvement in Restructuring: The Effects of Board Versus Managerial Controls and Characteristics," *Strategic Management Journal*, Vol. 14, 1993, pp. 33-50.

[38] Judge, W.Q. and Zeithaml, C.P., "Institutional and Strategic Choice Perspectives on Board Involvement in the Strategic Decision Process," *The Academy of Management Journal*, Vol. 35, 1992, pp. 766-794.

[39] Kankanhalli, A., Teo, H., Tan, B., and Wei, K.K., "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management*, Vol. 23, 2003, pp. 139-154.

[40] Karabacak, B. and Sogukpinar, I., "ISRAM: Information Security Risk Analysis Method," *Computers and Security*, Vol. 24, No. 2, 2005, pp. 147-159.

[41] Klein, A., "Audit Committee, Board of Director Characteristics, and Earnings Management," *Journal of Accounting and Economics*, Vol. 33, 2002, pp. 375-400.

[42] Knyazeva, A., Knyazeva, D., and Raheja, C., "The Benefits of Focus vs. Heterogeneity: An Analysis of Corporate Boards." Unpublished Working Paper: University of Rochester, 2009.

[43] Kor, Y.Y., "Direct and Interaction Effects of Top Management Team and Board Compositions on R&D Investment Strategy," *Strategic Management Journal*, Vol. 27, 2006, pp. 1081-1099.

[44] Kwon, J., Rees, J., and Wang, T., "The Association between Top Management Involve-

ment and Compensation and Information Security Breaches," *Journal of Information Systems*, Vol. 27, No. 1, 2013, pp. 219-236.

[45] Lipton, M. and Lorsch, J.W., "A Modest Proposal for Improved Corporate Governance," *Business Lawyer*, Vol. 48, 1992, pp. 59-77.

[46] Lorsch, J.W. and Maclver, E., *Pawns or Potentates: The Reality of America's Corporate Boards*. Boston: Harvard Business School Press, 1989.

[47] Monks, R. and Minow, N., *Corporate Governance*. Cambridge, MA: Blackwell, 1995.

[48] Olson, M., "The Rise and Decline of Nations." New Heaven, CT: Yale University Press, 1982.

[49] Pfeffer, J., "Organizational Demography," in *Research in Organizational Behavior,* L.L. Cummings and B.M. Staw (eds.). Greenwich, CT: JAI Press, 1983, pp. 299-357.

[50] Raheja, C.G., "Determinants of Board Size and Composition: A Theory of Corporate Boards," *Journal of Financial and Quantitative Analysis*, Vol. 40, 2005, pp. 283-306.

[51] Ranmachandran, S. and Rao, S., "Security Cultures in Organizations: A Theoretical Model," in: *Americas Conference on Information Systems*. Acapulco, 2006.

[52] Richardson, R., "2008 CSI Computer Crime and Security Survey," 2008.

[53] Robinson, G. and Dechant, K., "Building a Business Case for Diversity," *The Academy of Management Executive*, Vol. 11, 1997, pp. 21-31.

[54] Rosenstein, S. and Wyatt, J.G., "Outside Directors, Board Independence, and Shareholder Wealth," *Journal of Financial Economics*, Vol, 36, 1990, pp. 175-191.

[55] Shleifer, A. and Vishny, R.W., "A Survey of Corporate Governance," *The journal of finance*, Vol. 52, No. 2, 1997, pp. 737-783.

[56] Siponen, M. and Iivari, J., "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems*, Vol. 7, No. 7, 2006, pp. 445-472.

[57] Smith, K.G., Smith, K.A., Olian, J.D., H.P. Sims, J., O'Bannon, D.P., and Scully, J.A., "Top Management Team Demongraphy and Processes: The Role of Social Integration and Communication," *Administrative Science Quarterly*, Vol. 39, 1994, pp. 412-438.

[58] Straub, D. and Welke, R., "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, 1998, pp. 441-469.

[59] TIAA-CREF, *Policy Statement on Corporate Governacne*. New York, 1997.

[60] Walsh, J.P. and Seward, J.K., "On the Efficiency of Internal and External Corporate Control Mechanisms," *The Academy of Management Review*, Vol. 15, No. 3, 1990, pp. 421-458.

[61] Wang, T. and Hsu, C., "Board composition and operational risk events of financial institutions," *Journal of Banking and Finance*, Vol. 37, 2013, pp. 2042-2051.

[62] Wang, T., Kannan, K., and Rees, J., "The Association between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research*, Vol. 24, No. 2, 2012, pp. 201-218.

[63] Williams, K.Y. and O'Reilly, C.A., *Demography and Diversity in Organizations*. Greenwich: JAI Press, 1998.

[64] Yayla, A.A. and Hu, Q., "Determinants of Cio

Compensation Structure and Its Impact on Firm Performance," *Proceedings of the 41st Hawaii International Conference on System Sciences*), 2008.

[65] Yermack, D., "Higher Market Valuation of Companies with a Small Board of Directors," *Journal of Financial Economics*, Vol. 40, 1996, pp. 185-211.

[66] Zenger, T.R. and Lawrence, B.S., "Organizational Demography: The Differential Effects of Age and Tenure Distributions on Technical Communication," *The Academy of Management Journal*, Vol. 32, No. 2, 1989, pp. 353-376.

## ◆ About the Authors ◆

Carol Hsu

Carol Hsu is a Professor in the Department of Information Management at National Taiwan University. She holds a Ph.D. in information systems from the London School of Economics and Political Science. Her current research interests focus on the organizational and cultural issues related to information IT diffusion in the financial industry and information security management. Her work has been published in the *MIS Quarterly, Information Systems Research, European Journal of Information Systems* and *Communications of the ACM. She also serves as Associate Editor for Information Systems Journal* and *Information and Management.*

Tawei Wang

Tawei Wang is currently an Assistant Professor of Accounting and Accuity LLP Accounting Faculty Fellow at Shidler College of Business, University of Hawaii at Manoa. He received his Ph.D. from Krannert Graduate School of Management, Purdue University in 2009. His research interests are information security management and IT management. His papers have appeared in several leading journals, including *Information Systems Research, Decision Support Systems, European Journal of Information Systems, Information and Management, Information Systems Journal, Journal of Accounting and Public Policy, Journal of Banking and Finance, Journal of Information Systems, Journal of Organizational Computing and Electronic Commerce*, among others. He received two Shirley M. Lee Research Awards at Shidler College of Business in 2013 and 2014, and several teaching awards including the Krannert Distinguished Teaching Award, the Krannert Outstanding Teaching Award, and Purdue Graduate Student Award for Outstanding Teaching.

Submitted : May 02, 2014
1st revision : August 07, 2014
2nd revision : October 07, 2014
Accepted : November 26, 2014