Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2010 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2010

The Impact of Board Structure on Information Security Breaches

Tawei Wang
National Taiwan University, twang@ntu.edu.tw

Carol Hsu
National Taiwan University, carolhsu@ntu.edu.tw

THE IMPACT OF BOARD STRUCTURE ON INFORMATION SECURITY BREACHES

Tawei Wang, Department of Accounting, National Taiwan University, Taipei, Taiwan, twang@ntu.edu.tw

Carol Hsu, Department of Information Management, National Taiwan University, Taipei, Taiwan, carolhsu@ntu.edu.tw

Abstract

This paper investigates the association between the board structure of a firm and the possibility of information security breaches. Building on the agency theory and resource dependence theory, we hypothesize that the board structure could affect the guidance and advice capability of the board on the executives' decision of information security management. Our results show that the board size and the number of independent directors could increase the possibility of security breaches while the average and heterogeneity of age/tenure could reduce it. Our findings shed lights on the crucial role played by the board when managing information security risks in organizations.

Keywords: information security, board structure, breach announcement, resource dependence.

1 INTRODUCTION

While the advance and commoditization of information communication technology (ICT) bring modern organizations the opportunity to achieve and maintain competitiveness in the marketplace, organizations are increasingly facing challenges to combat the increasing numbers of external and internal threats that exploit organizational vulnerabilities (CSI/FBI 2008; Deloitte 2009). The growing involvement of regulatory thinking also brought a profound impact on the discursive process about risk management and corporate governance in organizations, such as the Sarbanes-Oxley Act (SOX) and Basel II. In the information security management literature, studies on organizational aspects are "limited but emerging" (Ransbotham and Mitra 2009, p.122). Our assessment of the literature indicates that most organizational approaches in this area are dominant in the analysis of security policy development, risk management, and security effectiveness/misuse. In our view, despite pointing to the significance of top management support in some studies, discussion on the impact of organizational structure, such as the board structure and heterogeneity, on the possibility of information security breaches is still lacking. In accordance with the corporate governance literature, we argue that the board of directors play a crucial role in influencing managerial actions in managing risk and developing policy, which has a consequent impact on the effectiveness of information security management program or the possibility of information security breaches in the organization. Therefore, our research objective is three-fold. First, we discuss the conceptual argument about the relation between the board structure and information security management. Second, we attempt to identify major variables and develop hypotheses on how the board composition might influence the possibility of information security breaches in the organization. Third, we empirically test the proposed hypotheses using the data of the *S&P 1500* firms in the *Risk Metrics* database between 1996 and 2008.

The remainder of the paper is organized as follows. In the next section, we discuss the theoretical perspectives that are relevant to the board structure and information security management, which is followed by the development of hypotheses. We continue with the description of research methodology deployed in this study and the discussion of empirical findings. Concluding remarks include the discussion of contributions and implications of our research.

2 THEORETICAL FRAMEWORK AND HYPOTHESES

In this section, we present our conceptual framework linking the relevance between the board structure and the effectiveness of information security management from prior literature.

In information systems literature, information communication technology (ICT) has known for its strategic importance for organizational survival and success (Porter 1980). However, as mentioned earlier, the widespread adoption of information technology infrastructure has recently brought managerial and scholarly attention on its side effect, i.e., the risks associated with the technology diffusion (e.g., Carr 2003; Ciborra 2006). Further assessing the information security management literature, we found that the organizational aspect of research is still relatively limited compared with the research on its technical counterpart. Within the organizational perspective, the majority of studies on risk management have centred on the description of various frameworks (Bandyopadhyay et al. 1999; Baskerville 2008; Eloff 1993; Karabacak 2005; Mattord and Wiant 2008; Rainer et al. 1991) or its the implementation process and its effectiveness (Dhillon and Backhouse 1996; Straub 1990; Straub and Nance 1990; Straub and Welke 1998). However, if one follows the arguments put forward by Carr (2003) and Ciborra (2006), together with the legislative development, the strategic importance of effective information security management is apparent and should be addressed in the research. With the emphasis on the strategic imperative, we further contend that the board composition and structure hence become important in this context as they are influential in a firm's strategic direction and performance. To the best of our knowledge, no research yet has examined the relation between the board structure and the effectiveness of information security management.

The design and composition of the board is widely discussed and examined in the area of corporate governance research (e.g., Baysinger and Butler 1985; Core et al. 1999). Drawing from the agency theory, the board is an important control mechanism that serves to protect the interest of shareholder from the self-interested executives (Shleifer and Vishny 1997; Walsh and Seward 1990). However, others have adopted the resource dependence theory and considered the value of directors as the provision and access to other resources beyond the organizational boundary. In this research, we consider that both theoretical perspectives are highly relevant to the effectiveness of information security management. First, unlike other organizational investment, organizational spending on information security seldom generates strategic return on organizational performance. Although many organizations have implemented information security over the past decade (e.g., Dhillon and Backhouse 2001; Cavusoglu et al. 2005; D'Arcy 2009; Gordon, et al 2006; Hsu 2009; Ransbotham and Mita 2009), it is still difficult to persuade top management to invest the appropriate amount in information security programs. Thus, to protect the reputation and prevent the financial loss caused by security breaches, the board is imperative in ensuring sufficient managerial attention and investment in information security. Second, given the swift change in technology and business environment, organizations constantly face the challenges of dealing with uncertain threats that might exploit organizational vulnerabilities. From the viewpoint of resource dependency theory, the value of the board then lies in the provision of professional experience and opinions to enhance the managerial capacity in developing a sound risk management approach. Put together, we have developed the correspondent hypotheses as detailed below.

First, prior literature regarding board structure has focused on the size of the board (e.g., Beasley 1996; Dalton et al. 1999). Based on our discussion in the previous paragraph, 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. From this viewpoint, the size of the board can reduce the possibility of information security breaches. However, in the context of information security, the uncertainty faced by a firm changes rapidly, a larger group of directors can also complicate and slow down the decision-making process at the board meeting (e.g., Olson 1982). That is, a larger board might hinder the organization's capability of responding to the environmental change (e.g., Goodstein et al. 1994; Harrison 1987). This implies that the size of the board could 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 possibility of information security breaches.

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

Second, the volatile technology and business environment often limits the capability of top management in making a well-informed decision. As the resource dependence theory indicates, the composition of the board plays an important role in sourcing the knowledge to support the corporate information security management. In the literature, age and tenure are the two factors that are commonly discussed about the composition of the board (e.g., Carter et al. 2002; Finkelstein and Hambrick, 1989; Johnson et al. 1993; Robinson and Deschant 1997). The main argument in this stream of literature is that the age and tenure is associated with the director's experience and capabilities. In our context, the older the directors are and/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. On the other hand, the heterogeneity of age/tenure allows the board to have a diversity of information and a wide variety of viewpoints (e.g., Johnson et al. 1993; Wiersema and Bantel 1992) which could also negatively associated with breaches. Same as the argument presented earlier, the diversity on age/tenure could reduce the communications among the directors (e.g., Zenger and Lawrence 1989) and hinder the decision making which could oppositely increase the possibility of breaches. Similarly, since we are not able to determine the impact of the heterogeneity of age/tenure on the possibility of breaches, we have two competing hypotheses for the empirical test. Formally,

Hypothesis 2. The average age/tenure of the directors is negatively associated with the possibility of information security breaches.

Hypothesis 3a. The heterogeneity of age/tenure of the directors is positively associated with the possibility of information security breaches.

Hypothesis 3b. The heterogeneity of age/tenure of the directors is negatively associated with the possibility of information security breaches.

Another rationale concerning the value of the board is their link to outside resources and connection to the external environment (e.g., Hillman and Dalziel 2003). The link is developed through the set-up of independent directors. We found that the independent directors serve different purposes depending on what theoretical lens was deployed. One school of thoughts focuses on independent directors from the perspective of agency cost or monitoring cost such as Forker (1992), Klein (2002), Raheja (2005), and Drymiotes (2007). From the resource dependence perspective and in the context of information security, 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. Accordingly, as the number of independent directors increases, the internal knowledge might not be enough to guide the executives risk managing behavior.

Hypothesis 4. The number of independent directors is positively associated with the possibility of information security breaches.

3 SAMPLE AND RESEARCH MODELS

3.1 Data Collection and Measures

In order to approach our research questions, we used all the *S&P 1500* firms from 1996 to 2008 as our sample. The data of the board of the directors was collected from the *Risk Metrics* database. From the database, we calculated the number of directors and the number of independent directors for each firm-year. We also gathered the information about age and tenure for each director for each firm-year.

We then identified information security breach announcements from 1996 to 2008 in the major media outlets. 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 for 13 different keywords as indicated in prior literature (e.g., Campbell et al. 2003; Garg et al. 2003; Wang et al. 2009). From the details of these information security breach announcements, we carried out an exercise of cross-check with the sample of *S&P 1500* firms. If a firm in our sample had breach announcements, we coded the variable *Breach* as 1, 0 otherwise. The resulting sample size is 3,034 and consists of the firms from 63 industries.

3.2 Measures and Research Models

To operationalize our research objective, we decide to use the average amount for each measure in our sample period as detailed below. The average amount also helps us control the fluctuation across years. For Hypothesis 1, we calculated the average number of directors for each firm from 1996 to 2008 (*BSize*). For Hypothesis 2, we first calculated the average age (in years) and tenure (in days) for each firm year. Then we average again what we obtained above through our sample period (*avgAge* and *avgTenure*). For Hypothesis 3, we use 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*). For Hypothesis 4, the average number of independent directors was calculated. Last, we control for firm size (*CSize*, in millions) for our analysis.

We have missing values when we search the *S&P 1500* firm in the *Risk Metrics* database. Accordingly, there are fewer observations for the board structure measures which result in a total sample size of 2254. Note that the size of the firm (*CSize*) is positively and significantly correlated with board size (*BSize*) and the size of independent directors (*IBSize*) (0.625, $p < 0.01$ and 0.548, $p < 0.01$ respectively). Also, as expected, the board size (*BSize*) and the size of independent directors (*IBSize*) are highly correlated (0.799, $p < 0.01$). We recognize that such a correlation could be problematic when including these variables in the same model. Therefore, we take the residuals by regressing the size of the firm (*CSize*) on the board size (*BSize*) as an orthogonal measure for our analyses as presented in the following section. In addition, we will have two separate models for the board size and the size of independent directors.

Based on our measures, we use Equation (1) and Equation (2) below to test our Hypotheses. The dependent variable for these equations is *Breach*. In these two equations, other variables are those defined earlier, where the β_j are the coefficients and ε_1 and ε_2 are the residual terms. We estimate the coefficients using the logistic regression model.

$$Breach_i = \beta_0 + \beta_1 CSize_i + \beta_2 BSize_i + \beta_3 avgAge_i + \beta_4 avgTenure_i + \beta_5 CVAge_i + \beta_6 CVTenure_i + \varepsilon_{1i} \quad (1)$$

$$Breach_i = \beta_0 + \beta_1 CSize_i + \beta_2 IBSize_i + \beta_3 avgAge_i + \beta_4 avgTenure_i + \beta_5 CVAge_i + \beta_6 CVTenure_i + \varepsilon_{2i} \quad (2)$$

4 ANALYSIS AND RESULT

The results are given in Table 1. For Equation (1) (the second column in Table 1), all the variables are significant except the average tenure of the directors (*avgTenure*). The significant positive coefficient (0.2466, $p < 0.01$) for the variable *BSize* supports our Hypothesis 1a that it is more likely to have security breaches when the size of the board is larger. This presents an interesting finding compared to the existing literature on board size and firm performance. In the management literature, scholarly evidence suggests that board size tends to positively associated with the firm performance and could provide more external resources to the firm (e.g., Daily and Johnson 1997; Dalton et al. 1999; Gilson 1990; Pfeffer 1978). A large board can provide a stronger governance power which would reduce the dominance of managers and improve decisions (e.g., Zahra and Pearce 1989). Nevertheless, from the information security management perspective, the findings shed some lights on how to balance the pool of knowledge and the speed of decision-making required in managing information security risks. A larger board size might offer the merit of knowledge pool on the other hand could hinder the quality and process of decision-making. The quality of decision regarding information security in turn affects the effectiveness of security management and the firm's future uncertainty. Our results offer the empirical evidence that when the board size grows, the benefit of accessing to a diverse knowledge might become counterproductive from the standpoint of decision-making quality.

The above finding suggests an important theoretical thinking in effective information security management, that is, board size might not be the answer but the board composition matters (e.g., Knyazeva et al. 2009). In our analysis of board trait, the results indicate that the older the directors of the board, the smaller the possibility of breach (the coefficient of *avgAge* is -0.1183, $p < 0.01$ for Equation (1) and -0.1202 for Equation (2), $p < 0.01$). Focusing on the issue of board heterogeneity, the results for Equation (1) in Table 1 also support Hypothesis 3b (the coefficient of *CVAge* is -0.0453 for Equation (1), $p < 0.01$ and -0.0971 for Equation (2), $p < 0.10$; the coefficient of *CVTenure* is -0.2854, $p < 0.01$ and -0.3448, $p < 0.05$ for Equation (1) and (2) respectively). The result confirms the idea of "board capital" in prior studies (Hillman and Dalziel 2003). In particular, the board provides important expertise and skills to the provision of advice and counsel (e.g., Baysinger and Butler 1985; Gales and Kesner 1994). In addition, prior literature suggests that the heterogeneity within a group can reduce the possibility of inertia (e.g., Kiesler and Sproul 1982) and can reduce social cohension of the board (Michel and Hambrick, 1992). Heterogeneity tends to offers positive contribution to the management of the firm (Hambrick and Chen 1999; Wiersema and Bantel 1992). In our security

context, our finding suggests that experience plays an important role when facing security risks. 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 can preserve the confidentiality, integrity and availability of information in organizations. All these tasks require an enterpris-wide implementation and demand the talences and skills of management to executive them well. Furthermore, the depth of managerial experiencs from the board becomes singinficantly invaluable to the top managemnt team.

Variable	Equation (1)	Equation (2)	
Intercept	2.2252	**3.4542****	
CSize	**1.6752*****	**1.6638*****	
BSize	**0.2466*****		H1a supported
IBSize		**0.2805*****	H4 supported
avgAge	**-0.1183*****	**-0.1202*****	H2 supported
avgTenure	0.0000	-0.0000	
CVAge	**-0.0453*****	**-0.0971***	H3b supported
CVTenure	**-0.2854*****	**-0.3448****	
Model Chi-Square	188.55	183.76	
Percent Concordant	80.30	79.40	
Pseudo R^2	0.08	0.08	
N	2254	2252	
*** significant at 1% ** significant at 5% * significant at 10%			

Table 1. Results

For Equation (2) (the third column in Table 1), the result supports Hypothesis 4 that the number of independent directors is positively associated with breaches (the coefficient of *IBSize* is 0.2805, $p < 0.01$). Prior literature has shown that though outside directors could provide their experience and outside resources to the firm (e.g., 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 (e.g., Baysinger and Hoskisson 1990; Lorsch and MacIver 1989). In our information security context, it is inevitable to understand how a firm's strategy interacts with its environment and its capabilities (Applegate et al. 2009). Accordingly, the board needs to have more internal knowledge of value and risk when facing information security challenges. Therefore, the guidance function of the board is more important than the monitoring function in the security context.

5 IMPLICATION AND CONCLUSIONS

This study focuses on the guidance role played by the board of directors of a firm and investigates how the board structure would affect the effectiveness of security management which is proxied by the possibility of breaches. Our results suggest that the size of the board could hinder the quality of decision while the average age and the heterogeneity of age/tenure of the board could enrich the viewpoints the managers have when setting security policies. Furthermore, different from the prior literature, the number of independent directors becomes an indicator of how well the internal information about daily business the board can have and the management of information security.

This paper highlights the need for the consideration and investigation into the impact of the board structure on the effectiveness of information security management in organizations. We extend our empirical support to the conceptualization of 'duality of risk' (Ciborra 2006) and IT as infrastructure (Carr 2003) in organizations. That is, the board of directors does not only affect the organizational performance of the firm as indicated by prior literature, thy play an important role in information security management in organizations. From this angle, we add values to the existing literature on the organizational aspects of IS security. Our early work here presents exploratory results on the relationship between the board structure and information security breaches, but further work is needed to examine other aspects of the board structure and information security management. For example,

future studies can look into the relevance of different types of resources and its impact on organizational effectiveness of information security management.

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 management. 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. 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.

In summary, this research argues for the strategic imperative of board composition on the effectiveness of information security management in organizations. We further 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

Applegate, L. M., Austin, R. D. and Soule, D. L. (2009). Corporate Information Strategy and Management: Text and Cases. McGrawHill.

Baysinger, B. D. and Butler, H. N. (1985). Corporate Governance and the Board of Directors: Performance Effects of Changes In Board Composition. Journal of Law and Economics, and Organization, 1, 101-124.

Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market. Journal of Computer Security, 11, 431-448.

Carr, N. G. (2003). IT Doesn't Matter. Harvard Business Review, May, 41-49.

Carter, D. A., Simkins, B. J. and Simpson, W. G. (2003). Board Governance, Board Diversity, Firm Value. The Financial Review, 38, 33-53.

Ciborra, C. (2006). Imbrication of Representations: Risk and Digital Technologies. Journal of Management Studies, 43, 1339-1356.

Core, J. E., Holthausen, R. W. and Larcker, D. F. (1999). Corporate Governance, Chief Executive Officer Compensation, and Firm Performance. Journal of Financial Economics, 51, 371-406.

Dalton, D. R., Daily, C. M., Johnson, J. L. and Ellstrand, A. E. (1999). Number of Directors and Financial Performance: A Meta-Analysis. Academy of Management Journal, 42, 674-686.

Demsetz, H. and Lehn, K. (1985). The Structure of Corporate Ownership: Causes and Consequences. Journal of Political Economy, 93, 1155-1177.

Dhillon, G. and Backhouse, J. (1996). Structures of Responsibility and Security of Information Systems. European Journal of Information Systems, 5, 2-9.

Drymiotes, G. (2008). Managerial Influencing of Boards of Directors. Journal of Management Accounting Research, 20, 19-45.

Ellstrand, A. E., Tihanyi, L. and Johnson, J. L. (2002). Board Structure and International Political Risk. Academy of Management Journal, 45, 769-777.

Garg, A., Curtis, J. and Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches Information Management & Computer Security, 11, 74-83.

Goodstein, J., Gautam, K. and Boeker, W. (1994). The Effects of Board Size and Diversity on Strategic Change. Strategic Management Journal, 15, 241-250.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Sohail, T. (2006). The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. Journal of Accounting and Public Policy, 25, 503-530.

Hillman, A. J. and Dalziel, T. (2003). Boards of Directors and Firm Performance: Integrating Agency and Resource Dependence Perspective. Academy of Management Review, 28, 383-396.

Ho, J. L. Y., Wu, A. and Xu, S. X. Corporate Governance and Returns on Information Techonology Investment: Evidence from an Emerging Market. Working Paper, University of California.

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

Johnson, R. A., Hoskisson, R. E. and Hitt, M. A. (2003). Board of Director Involvement in Restructuring: The Effects of Board Versus Managerial Controls and Characteristics. Strategic Management Journal, 14, 33-50.

Pfeffer, J. and Salancik, G. R. (1978). The External Control of Organizations: A Resource Dependence Perspective. Harper & Row, New York.

Porter, A. (1980). A Guidebook for Technology Assessment and Impact Analysis. North Holland, New York.

Raheja, C. G. (2005). Determinants of Board Size and Composition: A theory of Corporate Boards. Journal of Financial and Quantitative Analysis, 40, 283-306.

Ransbotham, S. and Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. Information Systems Research, 20, 121-139.

Richardson, R. (2008). CSI Computer Crime & Security Survey.

Straub, D. and Nance, W. (1990). Discovering and discipline computer abuse in organizations: a field study. MIS Quarterly, 14, 45-60.

Straub, D. and Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision-Making. MIS Quarterly, 22, 441-469.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. Information Systems Research, 1, 255-276.

Tohmatsu, D. T. (2009). Losing Ground 2009 TMT Global Security Survey.

Wang, T., Rees, J. and Kannan, K. (2009). The Association Between the Disclosure and the Realization of Information Security Risk Factors. Working Paper, Purdue University.

Wiersema, M. F. and Bantel, K. A. (1992). Top Management Team Demography and Corporate Strategic Change. Academy of Management Journal, 35, 91-121.

Williams, K. Y. and O'Reilly, C. A. (1998). Demography and Diversity in ORganizations. JAI Press, Greenwich.

Zenger, T. R. and Lawrence, B. S. (1989). Organizational Demography: The Differential Effects of Age and Tenure Distributions on Technical Communication. Academy of Management Journal, 32, 353-376.