Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors

Emergent Research Forum Paper

Md. Shariful Islam
Louisiana Tech University
msi011@latech.edu

Thomas Stafford
Louisiana Tech University
stafford@latech.edu

Abstract

As Information Technology has become increasingly important to the competitive position of firms, managers have become more sensitive to their organization's overall IT risk management. Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of cyber-attacks, ensuring the adequacy of a company's cybersecurity measures has become a key area of purview for the Board of Directors (BoD). To address this issue, staffing the Board with members who have significant security expertise might be one of the best protective mechanisms in an increasingly risky business environment, both from the perspective of sound corporate governance and in terms of sensible IT governance. We expect that high-tech firms are far likely to have Board members with security expertise, and we expect that the degree to which IT is a differentiator or primary value proposition in the firm will moderate the presence of security expertise at the Board level, and we also expect that internal audit capabilities with security expertise will tend to moderate between a firm's technological sophistication and security expertise at the Board level.

Keywords
Cybersecurity/security, Internal Audit, Value Proposition, Competitive Differentiator.

Introduction

Information Technology (IT) is fundamental to a firm's survival and growth (Bharadwaj 2000). As such, IT is increasingly being applied to a broad range of operational, managerial, and strategic tasks in organizations (Zmud et al. 1987). Yet, the use of IT is not uniform in its deployment across firms. Rather, the information economy metaphor suggests that use of IT can be driven by management's ability to recognize and exploit opportunities for applying IT-based products and services (Zmud et al. 1987). This suggests that the use of IT is a function of many factors, including strategies, competitive positions, and competitive advantages.

IT penetration refers to an organization's overall success in embedding IT within its work systems. It is assessed by examining the extent to which IT is being applied to an organization's operational control, managerial control, and strategic planning activities. An additional aspect of IT penetration not captured in Anthony's framework (Anthony 1965) is the application of IT directed at gaining competitive advantages (Learmonth 1984; Wiseman 1985). Similar to IT penetration, IT integration refers to the extent to which IT is embedded as the integral part of organizations. We use IT penetration and IT integration interchangeably; (Deloitte 2013b) identifies four basic level of IT integration in companies:

Level 01: Technology is needed to operate the business, but the company can function if systems fail.

Level 02: Technology is strategically blended with other capital for competitive advantage; important areas of the business depend on timely, accurate IT information.

Level 03: IT is a competitive differentiator that is often critical to business strategy.

Level 04: IT is explicit in the value proposition for the company, and timely, accurate information is critical.

As IT has become increasingly important to the competitive position of firms, managers have become more sensitive to their organization's overall IT risk management (Rainer et al. 1991). Recent news reports highlight losses incurred by companies because of unsophisticated IT usage, and this serves to focus attention on the importance of these systems to the organization.

The Institute of Internal Auditors (IIA 2015) recently identified the top 10 risk areas in technology, and these include cybersecurity, information security, IT systems development projects, IT Governance, outsourced IT services, social media use, mobile computing, IT skills among internal auditors, emerging technologies, and board and audit committee technology awareness. Of the several IIA-identified risks bearing the potential to adversely influence business performance, our focus in this study is on the critical factor of cybersecurity/information security and the related degree of security sophistication of the corporate Board and its audit committee necessary to deal with these critical issues.

Background:

Recent years are characterized by the transformation of business models in every industry, leading to extensive technology-supported automation on the part of both customers and companies. In view of this, businesses have an increasing need to maintain their technological sophistication, which is the preservation of confidentiality, data integrity, and information access control that has driven the management of cybersecurity/security threats and risks into boardroom (Lanz 2014).

Not long ago, the term 'cybersecurity' was rarely heard of or directly addressed at the Board level. The Commissioner of New York Stock Exchange (NYSE) noted that over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators (Aguilar 2014). He further noted that "given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be critical part of Boards of Directors."

A recent survey of more than 250 board members indicates that cybersecurity is a rising concern at the Board level, even surpassing compliance risk (Tysiac 2014). In an investigation of executive roles and compensation schemes, as associated with security breach occurrences (Kwon et al. 2013), it was found that security breaches are less common when IT executives are involved in corporate leadership, and when such technology consultants at the Board level are compensated based on behaviors rather than outcomes. Recognizing these findings, (Higgs et al. 2016) extrapolate the premise that involvement at the Board level has an important impact on the cybersecurity component of IT risk.

The number of data breaches reported by companies has been growing and is expected to continue to increase (DiPietro 2013). To this end, corporate audit committees are beginning to focus on the connection between cybersecurity and an organization's financial well-being. Fully 70 percent of investors are interested in reviewing firms' cybersecurity practices and nearly 80 percent would not likely consider investing in firms with a history of cyber-attacks (HBGary Inc 2013). For this reason, firms need to consider an Information Technology Governance (ITG) mechanism involving cybersecurity that can satisfy regulatory compliance and investor demand for information, while managing the risks surrounding breaches. A likely avenue to meet this requirement is through increasing the degree of IT expertise at the Board level, but it is important to investigate the factors that lead to this important outcome.

Hypotheses:

The degree of cybersecurity/security concerns, just as with the sophistication of IT use, is not the same across all organizations, even though all companies are increasingly under increasing threat of cyber-attacks (Aguilar 2014). Without a good understanding of the nature of IT and its integration into corporate strategy, it is difficult for companies to effectively reply to the rising cybersecurity threat. In organizations where IT is a fundamental element in competitive advantage (Level # 03, above) or where technology is an important aspect of the overall value proposition (Level # 04), it is appropriate to form an IT subcommittee at the Board level (Deloitte 2013b).

To address cybersecurity/security risks, a balanced Cyber-threat risk management capability is of vital importance. Characteristics of a mature cyber-threat risk management capability include the following components – communication, people, process, and technology (Deloitte 2013a). In terms of the "people" component, it is important that executives have the requisite background knowledge and current information to actively integrate cyber-threat risks into broader Enterprise Risk Management (ERM) decisions. In view of this, it is ever more important to have security expertise at the Board level.

(Aguilar 2014) noted that many Boards lack the technical expertise necessary to be able to evaluate whether management is taking appropriate steps to address cybersecurity issues. As a result, there are calls for mandatory cyber-risk education for directors (Johnson 2014). Others have suggested that Boards at least be composed of members with a good understanding of information technology issues that pose risks to the company. The first and most important strategy in managing cybersecurity is to ensure that the organization fully understands how technology facilitates the achievement of its business objectives and what its tolerance is for suffering technology-related losses (Lanz 2016). Of the four levels of IT integration identified (e.g., Deloitte 2013b), we focus on the Level 3 and 4 since we believe they are most susceptible to cyber-risk. To that end, we hypothesize:

H1: *High-tech companies are likely to have audit committee/board members with security knowledge.*

H1a: *The companies in which IT is a competitive differentiator (Level 3) are likely to have audit committee/board members with security expertise.*

H1b: *The companies in which IT is explicit in the value proposition (Level 4) are likely to have audit committee/board members with security expertise.*

Represented in graphical format:

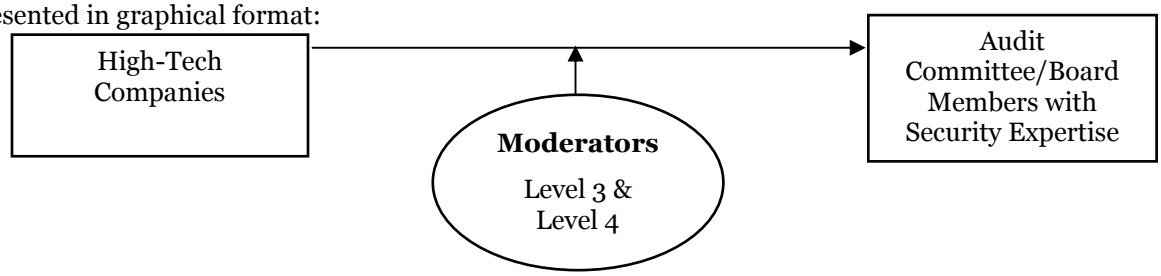

Figure 1

Cybersecurity/security risk is one of many risks enterprises face, and is a critical component of Enterprise Risk Management (ERM). Effective ERM is the product of multiple layers of risk defense (Deloitte 2015), but for effective risk management, organizations should institute and continually shore up three lines of defense: management, risk management and compliance, and internal audit. Internal audit should support the Board's need to understand the effectiveness of cybersecurity controls. A robust internal audit function provides objective assurance to the Board and executive management on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate.

Given that data security and privacy breaches can result in significant financial losses and marked reductions in market reputation for firms, the firm's BoD should be quite motivated to effectively assess and manage these risks. Keeping the audit committee apprised of emerging risks and effective ways to address them is a key role of the internal audit function (PwC 2012). Internal audit is the main conduit of for the provision of technology and security awareness to the Board and the Audit Committee (IIA 2015). Yet, even when companies have instituted the proper controls, failures are common. Tests have shown that even one day after learning how to avoid phishing scams, as many as 50% of employees will fall victim to them. This means that companies need to put into place a strong *third* line of defense. This is the assurance role that internal audit is uniquely positioned to master. Therefore, we hypothesize:

H2: *Having Internal Audit (IA) with security expertise will moderate the relation between high-tech companies and having security expert in audit committee.*

Graphically, we represent this hypothesis:

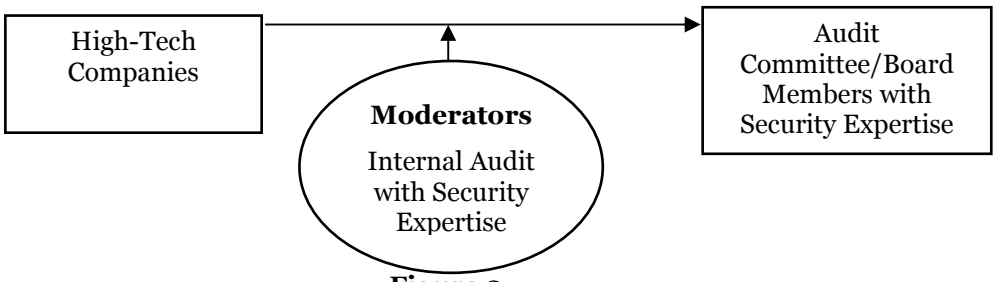

Figure 2

Research Methodology:

We have devised a means to test for the presence in companies of Board/audit members with the requisite security expertise, utilizing logistic regression. In line with previous research (Higgs et al. 2016), we establish control variables of SIZE, R&D, LEVERAGE, PROFIT and PAST_BREACH. The variable SIZE represents the size of the company, and we expect a positive coefficient estimate for this variable because we believe larger companies are more likely to have members with security expertise on their Board/Audit Committee. The variable R&D measures the extent to which organizations are likely to have intellectual property; the greater the intellectual property, the greater the probability of being the target of cyber-security attack. We also expect a positive coefficient for R&D.

The variable LEVERAGE represents the financial flexibility of companies; we believe that less financially flexible firms are less financially equipped to take have members with security expertise on their Board/Audit Committee. The term PROFIT measures the profitability of the firms, with profitable firms being more likely to have members with security expertise at the Board level, and we also expect a positive coefficient for this variable. The variable PAST_BREACH is a dummy variable, representing whether there have been past data breaches and we would expect a positive coefficient for prior breach disclosures. As primary variables of interest, we include the variables HIGH_TECH, COMPETITIVE_DIFFERENTIATOR, VALUE_PROPOSITION, INTERNAL_AUDIT, HIGH_TECH*COMPETITIVE_DIFFERENTIATOR, HIGH_TECH*VALU_PROPOSITION, HIGH_TECH*INTERNAL_AUDIT, INTERNAL_AUDIT*COMPETITIVE_DIFFERENTIATOR, and INTERNAL_AUDIT* VALU_PROPOSITION. The term HIGH_TECH will refer to those industries that are considered technology intensive, a factor which can easily be identified from public filings in order to develop a sample frame for analysis. We will then differentiate industries using two variables: COMPETITIVE_DIFFERENTIATOR and VALUE_PROPOSITION. COMPETITIVE_DIFFERENTIATOR refers to those companies in which IT is a competitive differentiator critical to business strategy (defined here as Level 3) and VALUE_PROPOSITION referring to those companies in which IT forms the key value proposition and in which timely and accurate information is critical (Level 4). INTERNAL_AUDIT is a dummy variable, indicating whether the companies have IA with security expertise or not. Additionally, different interaction variables were created to figure out the moderating effects. To that end, our model is:

$$\textbf{Prob (Members with Security Expertise = 1) = F [}\beta_0 + \beta_1 (\text{SIZE}) + \beta_2 (\text{R\&D}) + \beta_3 (\text{LEVERAGE}) + \beta_4 (\text{PROFIT}) + \beta_5 (\text{PAST\_BREACH}) + \beta_6 (\text{HIGH\_TECH}) + \beta_7 (\text{COMPETITIVE\_DIFFERENTIATOR}) + \beta_8 (\text{VALUE\_PROPOSITION}) + \beta_9 (\text{INTERNAL\_AUDIT}) + \beta_{10} (\text{HIGH\_TECH*COMPETITIVE\_DIFFERENTIATOR}) + \beta_{11} (\text{HIGH\_TECH*VALUE\_PROPOSITION}) + \beta_{12} (\text{HIGH\_TECH*INTERNAL\_AUDIT}) + \beta_{13} (\text{INTERNAL\_AUDIT*COMPETITIVE\_DIFFERENTIATOR}) + \beta_{14} (\text{INTERNAL\_AUDIT*VALUE\_PROPOSITION})] + \varepsilon$$

Conclusion

As IT has become increasingly important to the competitive position of firms, managers have become more sensitive to their organization's overall IT risk management. With the rapid advancement of technology, cybersecurity has become an increasingly challenging risk that Boards must address, through increasing the membership on the Board with IT security expertise in their portfolio, even advancing members with security expertise to the Board/Audit Committee. Security expertise at the Board level is

just a starting point in recognition of the seriousness of cybersecurity threats in today's business environment. Strong internal audit teams might moderate the deficiency of board security expertise, and the model we develop and propose can demonstrate that internal audit with security expertise might compensate for the absence of members with security expertise on Board/Audit Committee.

References

Aguilar, L. A. 2014. "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" (https://www.sec.gov/News/Speech/Detail/Speech/1370542057946).

Anthony, R.N. 1965. *Planning and control systems: A framework for analysis*. Harvard Graduate School of Business Administration, Cambridge, MA.

Bharadwaj, A. 2000. "A Resource-based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly* (24:1), pp.169-196.

Deloitte. 2013a. "Steps the C-suite and Board Can Take to Guard against Cyberthreats" (http://deloitte.wsj.com/riskandcompliance/2013/05/07/steps-the-c-suite-and-board-can-take-to-guard-against-cyber-threats/)

Deloitte. 2013b. "Evaluating IT Security: Issues for Audit Committees to Consider" (http://deloitte.wsj.com/riskandcompliance/2013/07/01/evaluating-it-security-issues-for-audit-committees-to-consider/)

Deloitte. 2015. "Cybersecurity: The changing role of audit committee and internal audit," Deloitte & Touche Enterprise Risk Services Pte Ltd.

DiPietro, B. 2013. "Cybercrime 2014: More Attacks, More Boardroom Scrutiny" (http://blogs.wsj.com/cfo/2013/12/03/cybercrime-2014-more-attacks-more-boardroom-scrutiny/)

HBGary Inc. 2013. "Cybersecurity Directly Affects Investor Attitudes, New HBGary Survey Finds" (http://www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html)

Higgs, J., Pinsker, R., Smith, T., & Young, G. 2016. "The relationship between board-level technology committees and reported security breaches," *Journal of Information Systems* (30:3), pp. 79-98.

Johnson, K. W. 2014. "Publicly Traded Companies Should Prepare to Disclose Cybersecurity Risks, Incidents" (http://www.bna.com/publicly-traded-companies-n17179885721)

Kwon, J., Ulmer, J. R., & Wang, T. 2013. "The association between top management involvement and compensation and information security breaches," *Journal of Information Systems* (27:1), pp.219-236.

Lanz, J. 2014. "Cybersecurity Governance: The Role of the Audit Committee and the CPA," *The CPA Journal*, pp. 6-10.

Lanz, J. 2016. "Communicating Cybersecurity Risks to Audit Committee," *The CPA Journal*, pp. 6-10.

Learmonth, B. I. 1984. "The Information System as a Competitive Weapon," *Communications of the ACM* (27:12), pp. 1193-1201.

PwC. 2012. "Fortifying Your Defenses the Role of Internal Audit in Assuring Data Security and Privacy" (https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-internal-audit-assuring-data-security-privacy.pdf)

Rainer, R. K., Snyder, C. A., & Carr, H. H. 1991. "Risk Analysis for Information Technology," *Journal of Management Information Systems* (8:1), pp.129-147.

The Institute of Internal Auditors (IIA). 2015. "Navigating Technology's Top 10 Risks: Internal Audit's Role" (http://theiia.mkt5790.com/Navigating_Technologys_Top_10_Risks/?webSyncID=ad198d79-4339-ec0a-2abb-4c8b921c8214&sessionGUID=3a377147-20a2-dc63-b3e7-2797d85899ba)

Tysiac, K. 2014. "Technology plays a role in board members' top two concerns" (http://www.cgma.org/Magazine/News/Pages/201410602.aspx)

Wiseman, C. 1985. *Strategy and Computers: Information Systems as a competitive Weapons*, Homewood, IL: Dow Jones- Irwin.

Zmud, R. W., Boynton, A. C., & Jacobs, G. C. 1987. "An Examination of Managerial Strategies for Increasing Information Technology Penetration in Organizations," in *Proceeding of International Conference on Information Systems*, Pittsburgh, PA, pp. 24-44.