CORPORATE GOVERNANCE EFFECTIVENESS AND CYBER SECURITY RISK ASSESSMENT AND MANAGEMENT

A Research Proposal

Submitted to:
The Cluster to Advance Cyber-Security and Testing (CAST)
The University of Memphis

By

Zabihollah Rezaee PhD, CPA, CMA, CIA, CGFM, CFE,
CSOXP, CGRCP, CGOVP, CGMA, CRMA
Thompson-Hill Chair of Excellence & Professor of Accountancy
Fogelman College of Business and Economics
300 Fogelman College Admin. Building
The University of Memphis
Memphis, TN 38152-3120

Joseph H. Zhang, PhD, CPA
Assistant Professor
Fogelman College of Business and Economics
300 Fogelman College Admin. Building
The University of Memphis
Memphis, TN 38152-3120

December 2016

EXECUTIVE SUMMARY

A growing incident of cyber hacking and security breaches of information systems (e.g., Sony, Targets, JPMorgan Chase, Home Depot) threats sustainability of many firms and cost the U.S. economy more than $100 billion annually (CSIS, 2013). Firms should take these threats seriously and improve their corporate governance and compliance and risk assessment and controls to effectively combat cyber hacking and cyber security breaches. Commissioner Luis A. Aguilar of the Securities and Exchange Commission (SEC) states that "The capital markets and their critical participants, including public companies, are under a continuous and serious threat of cyber-attack, and this threat cannot be ignored" (Aguilar, 2014). Regulatory initiatives and guidelines are being developed in assisting public companies and their directors and officers to understand, identify, assess and manage risks of corporate cybersecurity (NIST, 2014). Commissioner Aguilar suggests that boards of directors to oversee cybersecurity issues by ensuring management commitments to properly assess the cybersecurity threats and manage their risks (Aguilar, 2014).

We examine the association between the board oversight function and the likelihood of cybersecurity breaches and the link between corporate governance effectiveness and cybersecurity risk assessment and management. We construct a measure of the likelihood of reported information security breaches for the period from 2004-2016, using DataLossDB (http://www.datalossdb.org). We use the existence of the board committee and/or executive position for the firm "compliance and risk" as a proxy for the board oversight of cybersecurity. Dodd-Frank Financial Reform Act of 2010 requires firms to place a keen focus on compliance risk. Specifically, the Dodd-Frank

Act of 2010 requires large financial institutions (over $10 billion in assets) to have a formal board-level risk committee that oversees the identification and assessment of the institution's risk management (Dodd-Frank Act, 2010, Section 165). We also examine the effects of audit efforts in reducing the risk of cybersecurity.

THEORETICAL FRAMEWORK AND RESEARCH QUESTIONS

A growing number of public companies have experienced some version of cybersecurity hacking, cyber-attacks, or data breach as more than 1, 517 firms have reported cybersecurity risk as of June 29, 2014 compared to 1, 288 in 2013 and 879 in 2012 (Yadron, 2014). These breaches can adversely affect business activities, board practices, corporate governance measures, internal control effectiveness and firm's financial results and position (Wang and Hsu, 2010a and b; Gordon et al., 2016; Holder et al., 2016). The signaling theory can be used by firms to signal their commitment to combating cybersecurity attacks and providing reasonable assurance to their customers and suppliers about the security and integrity of their business model, operations and financial conditions. Research questions addressed in this research project are: (1) Can corporate governance effectiveness reduce the incidents of cybersecurity breaches? (2) Is there any association between corporate governance effectiveness and cybersecurity risk assessment and management? Do audit efforts reduce the risk of cybersecurity breaches?