The International Journal of Business Management and Technology, Volume 3 Issue 1 January - February 2019
ISSN: 2581-3889

Research Article Open Access

Effects of IT Governance Measures on Cyber-attack Incidents

Nick J. Rezaee, Student
University of California, Santa Cruz
1156 High Street
Santa Cruz, CA 95064,

Kingsley O. Olibe, PhD
Department of Accounting
College of Business Administration
Kansas State University
Manhattan, KS 66506-0113

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

ABSTRACT: Growing incidents of cyber hacking and security breaches of information systems (e.g., Sony, Target, JPMorgan Chase, Home Depot, Cathay Pacific Airlines) threaten the sustainability of many firms and costs the U.S. economy more than $100 billion annually. Business organizations should take these threats seriously and improve their Information Technology (IT) governance and compliance, and cybersecurity risk assessment and controls to effectively prevent cyber hacking and cybersecurity breaches. The existence and persistence of cyber-attacks has elevated expectations for boards of directors to exert greater risk and compliance oversight and for executives to develop and implement managerial strategies for risk management processes to combat cyber-attacks. This paper examines the importance and relevance of IT governance measures including the board oversight function and managerial risk assessment strategies in preventing cyber-attacks. This paper provides policy, practical and research implications.

Keywords: Cybersecurity; IT Governance; Board Oversight; Risk Assessment and management; IT investment and budget.

I. Introduction

The ever-increasing business complexity, corporate governance, and risk management, along with the growing number of cyber-attacks, necessitates the use of technology to prevent and detect their occurrences. A higher frequency of cyber hacks and security breaches of information systems (e.g., Sony, Targets, JPMorgan Chase, Home Depot, Equifax) threatens the sustainability of many firms and costs the U.S. economy more than $100 billion annually [01]. The Equifax (one of three major consumer credit agencies) cyber breach is considered to be one of the largest data breaches in history and expected to affect nearly half of the United States population [02]. Hackers were able to infiltrate the Equifax system between May and July of 2017 because of vulnerabilities in its website software that affect about 143 million people [02]. On October 24, 2018, Cathay Pacific Airlines disclosed cyber-attacks that affect more than 9.4 million travelers and following the announcement its stock tumbled nearly 7% and lost more than $200 million of in market value [03]. Global business organizations should take these threats seriously and improve their information technology (IT) governance measures, including board oversight and compliance, risk assessment, and controls, to effectively combat cyber hacking to prevent cybersecurity breaches. Several years ago, Commissioner Luis A. Aguilar of the Securities and Exchange Commission (SEC) stated 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" [04]. This statement is still relevant considering recent cyber-attacks.

Motivated by growing cyber-attacks and current initiatives in cybersecurity, we address IT governance measures designed to effectively assess, manage, and disclose cybersecurity risks. The existence and persistence of

cyber-attacks has elevated expectations for boards of directors to exert greater risk and compliance oversight, and for executives to develop and implement managerial strategies for risk management processes to combat cyber-attacks. We examine the importance and relevance of IT governance measures including the board oversight function, managerial risk strategies, and investment in IT in minimizing the likelihood of cybersecurity breaches. Specifically, we raise the following research questions: (1) Does the extent of investment in IT and the annual budget for operation technology (OT) and information technology reduce the likelihood of cyber-attacks? (2) Does the designated risk and compliance board committee or appropriate equivalent committee reduce the probability of cyber-breaches? and (3) Does the existence of a designated executive position (Chief Information Officer; Chief Risk Compliance Officer) affect reported cyber-breaches?

II. Institutional Background and Literature Review

1.1. Institutional Background

The National Institute of Standards and Technology (NIST) Cybersecurity Framework defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks" and cybersecurity risk management as "the process of identifying, assessing, and responding to risk." [05]. There are a variety of cyber risks ranging from total or partial shutdown of corporate operation to compromise corporate information. Cybercrime is broadly defined as "an intended illegal act involving the use of computers or other technologies" and it consists of initiating and spreading computer viruses, phishing, cyber-attacks, and stalking activities that take place in a virtual setting [06]. Corporate account takeover, one of the stealthiest and fastest types of cyber-attack, cost global corporations about $455 million in 2012, jumped to $523 million and was projected to reach $800 million by the end of 2016 [06]. Three risks associated with corporate account takeover are: (1) online banking of corporate business transactions; (2) lack of awareness of corporate executives regarding corporate account takeovers; and (3) inadequate and ineffective internal controls over the online banking process [06].

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 [07]. These breaches can adversely affect business activities, board practices, internal control effectiveness and firms' financial results and position [08] [09] [10] [11]. 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 [12]. A 2018 study by Comparitech investigates a large sample of cyber-attacks and find that: (1) the stocks of breached firms underperform the market; (2) finance and payment firms experience the largest drop in share price performance following a breach, whereas healthcare organizations were least affected; and (3) breaches that leak highly sensitive information (e.g., credit card and social security numbers) experience larger drops in share price performance than firms that leak less sensitive information [13].

In August 2017, the Office of Compliance Inspections and Examinations (OCIE) of the SEC released the results of its second cybersecurity examination initiative, which offers observations of industry cybersecurity practices and recommendations for best practices in implementing cybersecurity programs [14]. Three losses are associated with cyber-attack incidents [15]. The first is the direct economic loss consisting of the destruction of assets, loss of trade secrets, operational impairment, and cost of remedial measures. The second loss relates to reputational damages and lost revenue following the disclosure of cyber-attacks and the loss of negative impact on the trading price of the firm's securities. The final loss is any fines and sanctions levied on firms' that announce cyber-attack incidents by regulators.

Regulatory initiatives and guidelines are being developed to assist public companies, their directors, and their officers with understanding, identifying, assessing and managing the risks of corporate cybersecurity [05]. Commissioner Aguilar suggests that boards of directors need to oversee cybersecurity issues by ensuring management commitments to properly assess the cybersecurity threats and manage their risks [04]. The SEC released its "Commission and Guidance on Public Company Cybersecurity Disclosures" on February 26, 2018, which requires public companies to disclose their material cybersecurity risks and related policies, procedures, and controls to detect cyber-attacks [16]. Furthermore, the SEC issued a report on October 16, 2018 that highlights the risks associated with cyber-related frauds and requires public companies to establish proper internal control procedures to prevent these frauds [17]. The SEC investigated nine public companies that lost more than $100 million in cyber-related frauds (e.g., emails from fake executives and vendors) and indicated that such losses amount to more than $5 billion for public companies since 2013 [17]. The SEC report is intended to inform public companies about two types of email scams including emails from fake executives and emails from fake vendors and to require public companies to consider cyber-related threats when designing and maintaining their system of internal accounting controls [17].

2.2 Prior Research

Prior studies examine several IT governance measures intended to help firms, and their directors and officers understand, identify, assess, and manage the risks of corporate cyber-security [05]. In the United States, New York's cybersecurity regulations became effective in March 2017, which required national and international financial services firms to develop cybersecurity programs and policies, designate a Chief Information Security Officer (CISO), limit who has access to data or systems, assess and manage cybersecurity risks, and have a written incident response plan [18]. These initiatives and guidelines suggest that board risk oversight function, managerial strategies and adequate IT

investment and cybersecurity infrastructure could ensure the integrity of IT systems and effectiveness of cyber-infrastructure in dealing with potential cyber-attacks and cybersecurity breaches.

The International Standards Organization (ISO) 31,000 defines risk as an uncertainty that influences objectives. In the aftermath of 2007-2009 global financial crisis, concerns that public companies' boards and executives failed to properly oversee risk assessment and management have led policymakers [19], regulators, and standard-setters [20] to require that companies disclose their board risk oversight and managerial risk strategies. These external risk oversight and management requirements are consistent with the agency-based theory of board oversight function and management fiduciary duty [21] for effective risk oversight and managerial risk management processes that could identify, assess, and manage critical risks [22] including cyber-attack risks. Thus, the effective board risk oversight and managerial risk strategies are expected to improve cyber-attack risk management by reducing cyber-hacking incidents that benefit the firm and its stakeholders.

Contrary to the above agency-based theory of board risk oversight and managerial risk strategies and practices, the institutional theory, as supported by prior research, suggests that the board may not have adequate time, skills, and information for effective risk oversight ([23]; [24]). Managerial risk strategies may also be viewed as window-dressing (e.g., [25]) and thus not effective in reducing the risk of cyber-attacks in generating real economic benefit (e.g., [25]; [26]).

Prior studies address several research issues of the link between IT governance, board risk oversight and managerial risk strategies and risk management and informed risk-taking. On one hand, IT governance, board risk oversight and managerial risk strategies can improve risk assessment and management and thus reduce cyber-attacks (e.g., [27]; [28]; [29]; [30]). On the other hand, directors may not have sufficient skills, time, and information for effective risk oversight (e.g., [23]; [24]) and managerial risk strategies may be viewed as window-dressing (e.g., [25]). Prior research (e.g. [27]; [28]; [29]; [30]) finds effective board oversight over risk management strategies can improve risk management that could combat cyber-attacks. This paper contributes to the literature by examining whether IT governance measures including board oversight function, and managerial risk strategies are associated with incidents of cyber-attacks.

III. IT Governance Cyber-attacks Measures Relevant to Cyber-attacks

Business organizations and their boards, management as well as investors and regulators have expressed concerns about ever-increasing cyber-attack incidents and are interested in finding ways to guard against and prevent further occurrences by establishing and implementing effective IT governance. IT governance is a process of managing IT in achieving an organization's goals to ensure that IT resources support objectives and thus consists of measures and strategies to manage an organization's intellectual property, security and privacy and ensure compliance with all applicable rules, regulations and standards [31]. IT governance measures determine the security assessment and strategies for data and IT system specification and classification, the identification of operational procedures, and physical and technical risks to ensure the effective, monitored and value-added IT activities. Figure 1 depicts IT governance measures of board oversight, executive commitments, IT investment, IT operating budgets, IT risk assessment and IT control activities. The following sections examine the relevance and importance of IT governance measures in preventing, detecting and correcting cyber-attacks. In recent years, IT governance has received more attention from regulators and the investment and business community for many reasons: (1) the existence and persistence of cyber-attack incidents (Sony, Targets, JPMorgan Chase, Home Depot, Equifax, Cathay Pacific Airlines); (2) IT governance is now accepted as an important component of the overall corporate governance; (3) IT governance defines roles and responsibilities of the board of directors, management and personnel in establishing IT strategies, policies and procedures in achieving IT goals; and (4) IT governance aligns the IT strategy with the organization's objectives.

Insert Figure 1 Here

1.2. IT Board Oversight

Digital business creates information risk and security challenges that need to be addressed by directors and officers to satisfy the need for adopting innovative technology initiatives and protecting the organization from cyber-attacks. Directors should initiate and oversee IT governance framework that is tailored to the company's IT strategies and is flexible and realistic. IT governance frameworks should be established and implemented to ensure proper utilization of IT resources and processes in achieving the organization's technological goals and in aligning IT strategies with business strategies. The board of directors as the representative of shareholders is under pressure to ensure that their company complies with all applicable laws, rules, regulations and standards intended to protect confidential information, data utilization and retention, financial responsibility and accountability, cyber-attacks, and disaster recovery.

Given the importance of cybersecurity, IT risks and governance, it is likely that corporate boards either already have a director who is well versed in information technology and data security or are looking for one to help it better understand the company's IT risk profile. The Information Security Booklet of the Federal Financial Institutions Examination Council (FFIEC) suggests several cybersecurity oversight and management activities including the following: (1) existence of a risk compliance board committee or executive position such as "Chief Information Officer (CIO); (2) implementation and management of information security and business continuity programs by the designated executive or board committee; (3) annual report to the board of directors or designated board committee by management on the overall status of the business continuity programs and information security; and (4) the existence of

a budgeting process for information security investments, related expenses, and annual reviews with approval by the board of directors [32].

Specifically, boards of directors should: (1) exercise its strategic oversight of IT governance by understanding how critical information is, and the importance of information security to the organization; (2) review and approve investment in IT and related security systems to ensure IT resources support the organizational strategy and risk profile; (3) oversee the development and implementation of IT strategies and programs; (4) obtain and review reports from management regarding IT resources, strategies, activities, risk assessment, and cybersecurity risk; and (5) oversee the achievement of IT Governance objectives.

Boards can oversee managerial risk strategies and practices to obtain an understanding of risks inherent in managerial strategies for risk appetite and access timely information on risk appetite, risk response strategies, and effective risk assessment and management (e.g., [33] [34]; [20]) including cybersecurity risk. Risk oversight rules, regulations and standards (e.g., [19]; [20]) recommend board risk oversight committees assume risk oversight responsibilities. A stand-alone board risk committee is preferable in taking advantage of committee members' expertise and ensuring a proper focus of risk assessment and management (tone at the top).

A recent study suggests that 68 percent of surveyed boards of directors ask for increased senior executive involvement in board risk oversight [35]. A single committee, on the other hand, may not have the capacity and capability to oversee risk and the entire board must be responsible for risk oversight function. A study conducted by the National Association of Corporate Directors (NACD) finds that one-third of responding directors whose firms have risk oversight committees believe risk should be the responsibility of the full Board [24]. Thus, board risk oversight can impact managerial risk strategies and practices that could reduce cyber-attack opportunities. A stand-alone board risk committee can be used as a signal to regulators and investors, indicating the firm's commitment and tone at the top in assessing and managing risks. On the other hand, a risk oversight committee can be viewed as creating role confusion by overlapping with the oversight responsibilities of other board committees (e.g., audit committee).

1.3. IT Audit Committee

The audit committee is a standing committee of the board of directors in charge of overseeing corporate governance, financial reports, internal control assessment and management and audit functions. Technological advances, globalization, the evolving cybersecurity breaches and regulatory initiatives in recent years have created new oversight challenges for audit committees. Corporate stakeholders continue to have high expectations of audit committees for protecting against cyber-attacks. An effective audit committee requires collaboration among corporate governance participants including the audit committee, management teams, internal and external auditors, legal counsel and other third parties to combat cyber-attacks. As cybersecurity threats evolve, and their risks become more widespread, the audit committee's oversight can play crucial role in ensuring effective prevention, detection and correction of cyber-attacks. The audit committee should also oversee the proper disclosure of managerial risk strategies pertaining to cybersecurity. A recent EY report on cybersecurity-related disclosure indicates that 70% of Fortune 100 companies disclosed that their audit committees oversee cybersecurity matters and that the type and depth of cybersecurity disclosures varied widely suggesting the need for more effective audit committee oversight [42]. The audit committee effectively overseeing financial reporting, internal control and audit processes related to cybersecurity activities and their proper disclosure can improve investor confidence in public information. The audit committee and the entire board of directors should consider the following cybersecurity-related matters:

1. Whether and how IT governance measures are integrated into the overall corporate governance.
2. Whether and how cybersecurity risks are assessed and managed as integral component of the overall internal control system.
3. Whether adequate and effective control activities are designed and implemented in response to the assessed cybersecurity risks.
4. Whether and how often the board and the audit committee review managerial strategies dealing with cybersecurity matters and their proper disclosure.
5. Whether and how cybersecurity risks and related controls are disclosed to shareholders as required by the SEC regulations.

1.4. IT Executive Commitment

Management is primarily responsible for managing company activities and affairs for the benefit of its shareholders, including implementing the business vision, goals, objectives and innovative IT strategies and projects. The proper and effective implementation of IT strategies and projects requires management to design and implement robust IT governance measures. Management should secure its desired return on IT investments by improving product performance and integrity, customer satisfaction, brand reputation, operation effectiveness, reliable financial reports and regulatory compliance. IT governance should be implemented by the chief compliance and information office with support from the board of directors and other executives in the C-Suite and IT personnel. IT executives should conduct regular reviews of IT implementation processes to fine-tune IT strategies, programs and processes in meeting IT objectives.

IT executives should: (1) understand that IT-related risks including cybersecurity risks influence the operation and achievement of the organization's goals; (2) manage processes within IT to assess these risks; (3) accept responsibility for the effective operation of IT activities; (4) obtain authorization of proper IT investment from the board

of directors; (5) communicate IT activities and operations to the board of directors and shareholders; (6) realize the value delivered by IT and the risk that it imposes; (7) ensure that the IT infrastructure (technology, people, processes) can support expected business needs; (8) assess and manage critical IT risks particularly as related to cybersecurity and (9) design and implement adequate and effective controls for IT activities that address the related risks.

Managerial risk strategies and practices can effectively reduce the occurrence of cyber-attacks. However, recent centralization of operations and information system internet-based technologies, to improve cost efficiency and effectiveness across supply chains, creates security risks and high exposure to, and dependency on, the Internet that provides opportunities for cyber hackers to engage in rewarding cyber-attacks. Centralization across organization functions requires the use of sophisticated operations technology (OT) and information technology (IT) with related network infrastructure to connect geographically diverse functions. Thus, managerial risk strategies pertaining to both OT and IT securities and controls have become increasingly important under a centralized system to prevent hackers from penetrating the systems and engaging in costly cyber-attacks. However, many OT and IT security programs are old, underdeveloped, and outdated, consequently creating incentives and opportunities for cyber-attackers to penetrate these programs and engage in costly cyber hacking activities. Managerial risk strategies and programs are initially designed to identify the emerging cyber-hacks or information security threats and implement risk assessment and internal control procedures to immediately respond to security breaches.

Prior research shows that 32 percent of surveyed companies have designated a chief risk offer or an equivalent [43][35]. Other public companies have established board risk oversight committees. Prior research finds that: banks with a board risk oversight committee exhibited lower return on equity andbuy-and-hold returns during the financial crisis [36], a board risk committee is not linked to the bank's stock price or return volatility during the crisis period, and banks with a risk oversight committee or a risk/compliance officer experience higher Standard & Poor's risk management rating [37]. Public companies have recently established a board-level technology committee as an important component of their IT governance to signal their commitment in detecting and responding to cyber-attacks. However, Higgs et al. [38] find that firms with technology committees are more likely to experience cybersecurity breaches than those without such committees. Know et. al [39], and Wang et al. [40] report that including an IT executive in the top management team is negatively associated with the likelihood of information security breaches. The Dodd-Frank Financial Reform Act of 2010 requires firms to place a keen focus on compliance risk. Specifically, the Act 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 ([19], Section 165). The most prevailing challenge is the tone at the top by the board of directors in creating an appropriate risk assessment, which is integrated into strategic decision-making.

1.5. IT Risk Assessment and Management

One of the most important components of IT governance is to assess and manage cybersecurity risk as an integral part of IT security strategy. An appropriate level of tolerable and acceptable cybersecurity risk needs to be determined to ensure IT governance goal achievement and cybersecurity value. Enterprise risk management and enterprise-wide security strategies should be used to assess and mange cybersecurity risk and enable the company to be proactive and have value-added business solutions rather than being reactive in responding to crises. Examples of risks that need to be assessed and managed are: (1) the availability, accessibility, security, quality, reliability and continuity of IT services; (2) failure to respond to the real needs of the business; (3) challenges in properly defining IT processes and the related controls; and (4) lack of proper framework to evaluate IT controls, take remedial actions and communicate material IT control weakness to the board of directors. Several IT internal control assessment and management guidelines are currently being used including COBIT, ITIL, COSO, CMMI and FAIR [41]. COBIT and COSO are generally used for IT risk assessment and management, whereas ITI, CMMI and FAIR are usually employed to streamline IT services and operations, evaluating IT processes and assessing operational and cybersecurity risks. A single domain framework or an integrated framework can be used in assessing and managing IT risks and related controls. The company's ERM should focus on strategy and operating performance overseen by the audit committee and carried out by the internal audit function. Corporate gatekeepers including the audit committee, senior executives, and internal and external auditors should consider the following ERM activities pertaining to cybersecurity:

1. Are the company's ERM policies, procedures and practices overseen and approved by the board of directors?
2. Has management effectively assessed risks relevant to cyber-attacks and designed proper control activities in response to the assessed risks?
3. Has the company invested in IT resources to ensure effective operation of the ERM system?

3.5. IT Investment

The achievement of effective IT governance requires adequate IT investment in the personnel, information, and infrastructure of both hardware and software. Inadequate IT investment increases the likelihood of a breakdown in the IT processes as well as the occurrence of material cybersecurity risks; both of which can be detrimental to business operations and relationships with customers. Adequate IT investment can protect and guard against business risks. IT investment should be adequate in supporting the IT resources necessary in syncretizing processes and in complying with regulations intended to maintain data confidentiality and retention, disaster recovery, financial integrity and accountability. IT investment should be adequate in improving the quality and quantity of IT services, IT process and IT performance.

IT investment should be periodically evaluated to ensure proper support of the organization's strategic goals. Implemented OT and IT security programs are designed to identify security threats and cyber-attack information, as well as assess their risk and related internal controls to effectively respond to any security breaches. Any risk associated with cyber-attacks should be effectively assessed in a timely manner and proper information security strategies should be designed and implemented to combat these risks. Establishing an effective tone at the top concerning oversight strategies by the board of directors and management is vital in defending against cyber-attacks. Data is any organization is the most crucial asset that should be safeguarded because of the complex technology environment and cyber-attacks. The board of directors and senior executives should address the following questions:

1. Are IT investments adequate to effectively respond in a timely manner to evolving complexities in IT processes and related risks?
2. Are there appropriate risk strategies to assess and manage cybersecurity risks of complex IT resources?
3. Is managerial risk appetite aligned to the corporate culture and strategic priorities for IT investments and related cybersecurity?

3.6. IT Control Activities

Adequate and effective internal control activities should be developed and implemented by management in response to the assessed IT risks. The board of directors should also oversee the effective implementation of IT controls in achieving IT objectives. IT control activities should address the achievement of the following main IT strategies: (1) ensure the alignment of IT governance with overall corporate governance in effectively managing the company for the benefit of its shareholders; (2) confirm that IT investment creates maximum business value; (3) address the identified IT risks and ensure that IT processes are in place and function effectively to enable proper risk assessment and management; (3) determine that the IT capability and infrastructure supports current business requirements and expected future growth; and (4) verify compliance with all IT applicable rules, regulations, and standards. Control activities should have processes for incident response plan to document the occurrences of cyber-attacks incidents. Management should design and implement the breach response plan that meets approval of the board of directors. The implemented response plan should contain information on regulatory agencies (e.g., the SEC) that would be contacted in the event of a breach.

The SECin its cybersecurity disclosure guidance provides a more robust disclosure of cybersecurity risks, material breaches, and potential impacts on public companies, business, operations, and finances [17]. Wang et al. [40] find that the disclosed security-related risks are less likely to be associated with the future disclosure of security breaches and the capital market reactions to the security breach announcements are influenced by the nature of the preceding disclosure. TheErnst and Young (EY) Center for Board Matters conducted an analysis of the cybersecurity disclosure practices of Fortune 100 companies in 2018 in the United States and found a wide variety of disclosures pertaining to IT governance, the board oversight, and managerial risk assessment, suggesting that there is much opportunity for the improvement of cybersecurity [42]. The EY study indicates that: (1) investors' cybersecurity risk assessment and management is an integral component of the board's risk oversight function; (2) investors are expecting more disclosure regarding the board's oversight planning and strategies for risk management and IT investment; (3) the majority of companies disclose that cybersecurity is the most important risk overseen by the board; (4) management routinely reports to the board on cybersecurity risk issues; (5) at least one board-level committee, in many cases the audit committee, oversees cybersecurity matters; and (6) cybersecurity is considered as an important communication item with shareholders.

IV. Conclusion

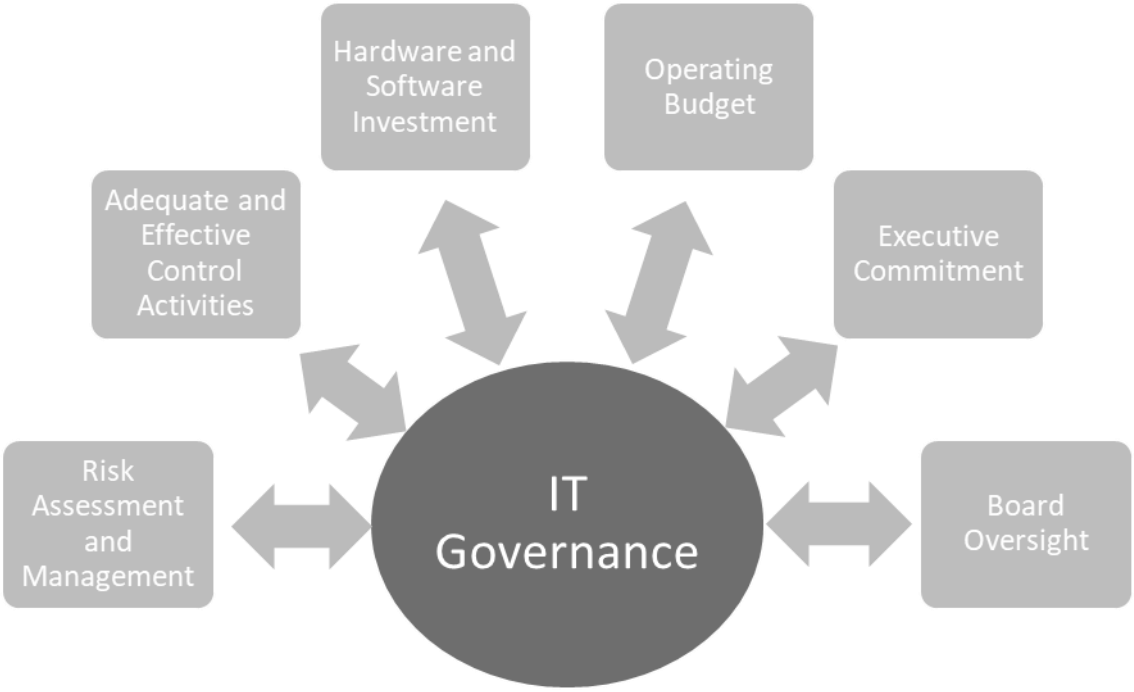
Recent cybersecurity breaches have eroded public confidence in the integrity of corporate activities, reliability of the financial reporting process, and quality of audit functions. Restoring the public confidence requires the coordinated effort of all corporate gatekeepers including the board of directors, executives, legal counsel, financial advisors, internal and external auditors, members of the accounting profession, audit firms, accountants, and academicians. Many companies are investing in new technologies, restructuring their business processes in response to evolving challenges and complexities in IT and related cybersecurity.

This study focuses on the role of IT governance measures as an integral part of corporate governance to assess and manage cybersecurity risk to improve the quality, reliability, and transparency of financial reports and bolster the credibility and effectiveness of related audit functions. This paper generates discussions on the importance of board oversight of cybersecurity matters, managerial assessment and management of cybersecurity risks, the effectiveness of IT governance in reducing cyber-attacks and proper disclosure of cybersecurity-related information to investors.

This paper provides policy, practical and research implications in several ways. First, it provides insight to the importance of risk governance, assessment and management for firms, particularly those that have experienced cyber-attacks. Second, it is relevant to policymakers, regulators and standard-setters in further establishing guidelines for public companies in addressing their cybersecurity risks and their proper disclosure. Finally, it contributes to the literature by addressing important research issues of cyber-attacks, cybersecurity, IT risks, and controls. It is expected that demand for and interest in a more robust communication with investors on cybersecurity-related matters continue to increase as cybersecurity threats and cyber-attacks continue to grow in occurrence. Future research should

empirically test the effectiveness of IT governance measures including board oversight, executive risk management and control activities in preventing cyber-attacks.

Figure 1



IT governance and its components

REFERENCES

[01] Center for Strategic and International Studies (CSIS). (2013). "The Economic Impact of Cyber Crime and Cyber Espionage," July 7, 2013. Available at csis.org/publication/economic impact-cybercrime-and-cyberespionage.

[02] Sternberg, L J. (2017). Surviving the Equifax Data Breach. AICPA Insights. September 14, 2017. Available at http://blog.aicpa.org/2017/09/surviving-the-equifax-databreach.html?cm_em=zrezaee@memphis.edu&cm_mmc=AICPA:CheetahMail-_-NewsUpdate-_SEP17-_-AICPANewsUpdate_A17SP136_IMTA#sthash.JuRiR7ZH.dpbs

[03] Garcia, M. (2018). Cathay Pacific Data Breach Highlights A Need To Change Airline Security Focus. Forbes, October 25, 2018. Available at https://www.forbes.com/sites/marisagarcia/2018/10/25/cathay-pacific-data-breach-highlights-a-need-to-change-airline-security-focus/#2b9a1a956b30

[04] Aguilar, L.A. (2014). Remarks by SEC Commissioner Luis A. Aguilar, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," June 10, 2014

[05] National Institute for Standards and Technology (NIST). (2014). "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," Feb. 12, 2014. Available athttps://www.temperednetworks.com/sites/default/files/resources/whitepapers/NIST-Compliance-Use-Case.pdf

[06] American Institute of Certified Public Accountants (AICPA). (2016). Top Cybercrimes White Paper. How CPAs Can Protect themselves and Their Clients. (December 2016). Available at http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/Cybersecurity/DownloadableDocuments/Top-5-CyberCrimes.pdf available at www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VEUaY_ldWvg.

[07] Yadron, D. (2014). Corporate boards race to shore up cybersecurity: Directors grapple with issues once consigned to teach experts. Wall Street Journal (June 29): 3.

[08] Wang, T., & C. Hsu. (2010a). "The composition of the top management team and the effectiveness of information security management." Americas Conference on Information Systems, Lima, Peru.

[09] Wang, T., & C. Hsu. (2010b). "The impact of board structure on information security breaches." Pacific Asia Conference on Information Systems (PACIS), Taipei, Taiwan.

[10] Gordon, L. A., M. P. Loeb, & T. Sohail. (2010). "Market Value of Voluntary Disclosures Concerning Information Security." *MIS Quarterly* 34 (3):567-594.

[11] Holder, A., K. Karim, K. Lin, & R. Pinsker. (2016). Do Material Weaknesses in Information-Technology related Internal Controls Affect Firms' 8-K Filing Behavior? *International Journal of Accounting Information Systems* 22: 26-43.

[12] Rezaee, Z. 2016. Business Sustainability Research: A Theoretical and Integrated Perspective" Journal of Accounting Literature,Volume 36, June 2016: 48–64

[13] Bischoff, P. 2018. Analysis: How data breaches affect stock market share prices (2018 update). Available.https://www.comparitech.com/blog/information-security/data-breach-share price-2018/

[14] Securities and Exchange Commission, Office of Compliance Inspections and Examinations (SEC/OCIE). (2017). National Exam Program, *Risk Alert: Observations from Cybersecurity Examinations* (Aug. 7, 2017) [hereinafter *OCIE Risk Alert*], *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[15] Gottlieb, C. (2018). Alert Memorandum: Untangling the tangled Web of Cybersecurity Disclosure requirements: A practical Guide. Available athttps://www.clearygottlieb.com/news-and-insights/publication-listing/market-abuse-regulation-impact-on-us-public-companies

[16] Securities and Exchange Commission (SEC). (2018a). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Release Nos. 33-1059; 34-82746, February 26, 2018. Available at https://www.sec.gov/rules/interp/2018/33-10459.pdf

[17] Securities and Exchange Commission (SEC). (2018b).Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements. Available at https://www.sec.gov/litigation/investreport/34-84429.pdf

[18] NYDFS. (2017). New York State Department of Financial Services: Cybersecurity Requirement for Financial Services Companies. March 1, 2017. Available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

[19] Dodd–Frank Wall Street Reform and Consumer Protection Act. (2010). 111th Congress Public Law 203, Government Printing Office, Washington, D., available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/html/PLAW-111publ203.htm.

[20] OECD. (2014). Risk Management and Corporate Governance, Corporate Governance. OECD Publishing. http://dx.doi.org/10.1787/9789264208636-en.

[21] Fama, E. (1980). Agency Problems and the Theory of the Firm. *Journal of Political Economy*, 88, 288-307.

[22] Caldwell, J. (2010). A Framework for Board Oversight of Enterprise Risk. *Canadian Institute of Chartered Accountants.*

[23] Ingley, C., & N. Van Der Walt. (2008). Risk management and board effectiveness. *International Studies of Management and Organization* 38 (3): 43-70. International Standards Organization. 2009. ISO 31000:2009, Risk Management— Principles and Guidelines. Geneva: International Standards Organization.

[24] National Association of Corporate Directors. (2013). Bridging effectiveness gaps: a candid look at board processes. Washington, DC: National Association of Corporate Directors.

[25] Westphal, J., & M. Graebner. (2010). A matter of appearances: How corporate leaders manage the impressions of financial analysts about the conduct of their boards. Academy of Management Journal 53 (1): 15-44. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[26] Saren, G., & J. Christopher. (2010). The association between corporate governance guidelines and risk management and internal control practices: Evidence from a comparative study. *Managerial Auditing Journal* 25 (4): 288-308.

[27] Tonello, M. (2007). Emerging governance practices in enterprise risk management. New York: The Conference Board, Report number R-1398-07-WG.

[28] Simkins, B., & Ramirez, S. (2008). Enterprise-wide risk management and corporate governance. *Loyola University Chicago Law Journal*, 39, 571-592.

[29] Adams, R. B. (2012). Governance and the financial crisis. *International Review of Finance* 12(1), 7-38.

[30] Gupta, P. & T. Leech. (2014). Risk Oversight: Evolving Expectations for Boards. New York: The Conference Board.

[31] Brisebois, R., G. Boyd, and Z. Shadid, August 2007, Canada - What is IT Governance? And Why Is It Important for the IS Auditor, The IntoSAI IT Journal, No. 25, pp. 30–35

[32] Federal Financial Institutions Examination Council (FFIEC). (2015). IT Examination Hand Book InfoBase. June 2015. Available at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx. and https://www.ffiec.gov/cyberassessmenttool.htm

[33] COSO. (2004). Enterprise Risk Management – Integrated Framework: Executive Summary. New York: Committee of Sponsoring Organizations of the Treadway Commission (September).

[34] COSO. (2009). Effective Enterprise Risk Oversight: The Role of the Board of Directors. New York: Committee of Sponsoring Organizations of the Treadway Commission (September).

[35] Beasley, M., B. Branson, & B. Hancock. (2015). 2015 Report on the Current State of Enterprise Risk Oversight. February 2015. Available at www.erm.ncsu.edu.

[36] Aebi, V., G. Sabato, & M. Schmid. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance* 36 (12): 3213-3226.

[37] Baxter, R., J.C. Bedard, R. Hoitash, & A. Yezegel.. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, 30 (4): 1264-1295.

[38] Higgs, J. L., R. E. Pinsker, T. J. Smith, & G. R. Young. (2016). The relationship between board-level technology committees and reported security breaches. Journal of Information Systems. Vol. 30, No. 3 (Fall 2016): 79-98.

[39] Know, J., J R. Ulmer, & T. Wang. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems.* Vol. 27, No. 1 (Spring 2013): 219-236.

[40] Wang, T., K N. Kannan, & J R. Ulmer. (2013) The Association Between the Disclosure and the Realization of Information Security Risk Factors. Information Systems Research 24(2):201 218.

[41] Long View. 2013. The 5 Domains of IT Governance. (October 22, 2013). Available at https://www.longviewsystems.com/it-governance/

[42] Ernst and Young (EY). (2018a). Center for Board Matters: Cybersecurity disclosure benchmarking. Available at https://www.ey.com/us/en/issues/governance-and-reporting/eycybersecurity-disclosure-benchmarking.

[43] Beasley, M., D. Pagach, & R. Warr. (2008). Information conveyed in hiring announcement of senior executives overseeing enterprise-wide risk management process. Journal of Accounting, Auditing and Finance 23: 311-332.