Chapter 10
Cybersecurity Oversight and Board Diversity: The Disclosure Paradigm

Manjula Shukla
SSSVS Government PG College, Chunar, India

Piyush Pandey
AMPG College, Varanasi, India

ABSTRACT

The study aims to determine how board diversity affects cybersecurity information disclosure for financial companies listed on S&P BSE 150. To create a CSD scorecard, the authors rely on past studies as well as SEC guidelines. The empirical research is based on data from 30 financial companies that were listed in India between 2013 and 2022. Panel data estimation technique was used to examine the connection between board diversity and CSD. The results demonstrate that CSD in Indian financial companies is in its infancy. CSD and independence diversity are significantly and favourably related. Gender diversity has no effect on CSD. Additionally, having an IT specialist on board considerably raises CSD levels and moderates the association between independence diversity and CSD, but does not successfully moderate the association between gender diversity and CSD. This study contributes to the literature through empirical evidence on the extent of CSD practises, relationship between board diversity and CSD, and the importance of an IT specialist on the board in defining CSD practises.

1. INTRODUCTION

A constant advancement in technology has brought about an era of internet-based transactions, mesh computing, data analytics and computerized methods, which have become an inherent part of the working system of businesses. Although information technology has proved to be a boon, it comes with a myriad of complexities, threats, and cybersecurity risks incidental to companies (SEC, 2018).

DOI: 10.4018/978-1-6684-8893-5.ch010

The Kotak Committee in 2017, heightened the role of the risk management committee and added cybersecurity to its purview. RBI in its recent circular mandated organizing training programs for the board of directors (B of D) of Indian banks to familiarize them and broaden their understanding of cybersecurity. The 2022 report of IBM Security Data Breach declares that for the financial year 2022, on average the data breach cost in India increased by 6.6 percent as of the financial year 2021 and reached ₹ 17.5 crores. In the year 2021, the major cybersecurity incidents pertained to compromised confidential information and unauthorized access. In a cyberattack case by Air India, the data files of millions of customers were leaked. In another instance, a data leak of the personal information of customers was witnessed from Domino's India's database (Chin, 2023). The major cybersecurity regulations currently administered in India are The Information Technology Act of 2000, which is the first cybersecurity law of India, NCS Policy, 2013, NCS Strategy, 2020, IT Rules, 2021, etc. CERT-In, NCIIPC, CRAT, SEBI, IRDAI, TRAI, DoT, etc. are the main cybersecurity regulatory bodies of India. In a ruling on a special petition of 2021, the Supreme Court of India declared that data theft and cyber-attacks are a crime under the IT Act of 2000 and the IPC. However, as the IPC is more than 150 years old, the IT Act, of 2000 is regarded as the prime cybercrime regulation in India (Chin, 2023).

Proper disclosures about the key aspects and functioning of a corporation are central to maintaining the public's confidence in the company. Companies have a continuous duty to promptly disclose information that investors would consider in making investment choices, including developments relating to a company's internal dynamics or that could otherwise have a bearing on the share price. The regulating agencies have frequently modified the mandatory disclosure standards for Indian corporations. However, the disclosures on cybersecurity have not been labelled as mandatory disclosure. Indian businesses are free to disclose cybersecurity issues as they see fit. The SEC 2011 proposed guidelines and regulations regarding cybersecurity disclosures by publicly traded companies in the USA. The regulations require companies to report cybersecurity incidents within a few hours of their occurrence through Form 8-K. The firms need to make periodic disclosures regarding the policies and procedures undertaken by the company to tackle and manage cybersecurity incidents, the role, expertise and oversight of the management and B of D in understanding and implementing cybersecurity functions, and make necessary cybersecurity disclosures in the annual report of the company through Form 10-K (Morse et al., 2018). There are currently no legislations in India requiring corporations to disclose cyber-risks in their annual reports. In a recent report by Yagnik, et al. (2022) there are relatively fewer disclosures in the annual reports of Indian companies on the topic of cyber-security, which indicates that this issue receives inappropriate attention from stakeholders.

The B of D, as per the agency hypothesis, act as the shareholders' agents. and as such, it is their responsibility to protect the shareholders' interests. The directors would take care to ensure that shareholders and other interested parties were informed of pertinent facts to do this. The value of diversity in management has long been appreciated since it allows for the inclusion of unique perspectives, diversity of thought, stakeholder representation, competitive advantage, inclusion of necessary skills, etc.

Several prior studies have investigated the effect of board diversity on various types of disclosures, which include GHG disclosure (Barg et al., 2022; Liao et al., 2015; Tingbani et al., 2020;), CSR disclosure (Ibrahim & Hanefah, 2016; Muttakin et al., 2015; Rao & Tilt, 2016), risk information disclosure (Bravo, 2018; Saggar et al., 2022), IC disclosure (Anifowose et al., 2017; Mooneeapen et al., 2022; Vitolla et al., 2020), carbon disclosure (Ben-Amar et al., 2017; Elleuch, 2022; Kılıç & Kuzey, 2019), etc. However, as per the researcher's knowledge, there is a narrow stream of research focusing on the impact of board