Corporate Governance and Cyber Security Effectiveness in Indian Corporations: An Analysis

Author: Prof. (Dr.) Seema Surendran[1]

Co-Author: Jahnavi M[2]

ABSTRACT

Corporate governance has evolved greatly with the rise of technology. The corporate sector is currently dealing with new cybercrime challenges as a result of technical advancement. However, fraudsters are creating new methods of data breaches that act as a risk to companies' reputation and competitive aspects. Cyber security has proven to be a key responsibility in companies, and the Board of directors have viewed it as an important cause of concern.

In India, data management and privacy have emerged as the central concerns of corporate governance. Government guidelines and company's policies can lead to complete eradication of cybersecurity concerns in India. The significance and requirement of cyber governance in ensuring cybersecurity are emphasized by this research. This paper analyses the cyber risks and the present laws that tackle the issue of cyber security risk in corporate governance. Further, the paper concludes with an analysis of the model policies and guidelines of leading companies for good corporate governance.

[1] Dr. Seema Surendran B.A LL. B, LL.M, MBA and Ph D degrees, Dr. Seema Specializes in Public International Law, Environmental Law and Criminal Law. Has an experience of over 22 years. Worked as faculty at Karnataka Lingayat Education Society's Law College Bangalore, Worked as Principal at Sri Kengal Hanumanthaiah Law College, Golden Valley Education Trust, K G F and BMS college of Law Bangalore. Assistant Professor at Amity Law School Noida, Amity University Uttar Pradesh. Worked as Associate Professor and Associate Dean (Academics) at Vivekananda Institute of Professional Studies (VIPS) Guru Govind Singh Indraprastha University, Delhi and presently working as Professor with CMR School of Legal Studies, CMR University Bangalore. Has attended a number of national and international seminars and holds number of publications to her credit.

[2] Jahnavi M is a resident of Bengaluru, currently pursuing LL.M in Commercial Law from CMR University, School of Legal Studies. She has completed her bachelors of law (BCOM LLB) from St Joseph's College of Law and comes with an experience of interning at top law firms in Bengaluru.

Keywords: Corporate governance, Cybersecurity, Board of directors, Government guidelines, Cyber risk.

I. INTRODUCTION

Corporate governance procedures are crucial in assisting businesses in recognizing and controlling risks. Businesses can mitigate risks to their finances, operations, and reputation by putting in place strong governance policies and procedures. Although a company cannot completely avoid risks, effective governance can lessen their effects when they do arise. In order to improve corporate governance in any organization, board members should place a high priority on risk management.

Corporate Governance has defined been by Organisation for Economic and Corporate Development (OECD), as involving a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the mechanism by which the company's objectives are set, and the means to achieve those objectives and track performance are decided."[3]

Corporate governance establishes guidelines and expectations for stakeholder relations, organizational performance, activity monitoring, and regulatory compliance. Corporate governance can offer companies enhanced protection against potential losses resulting from misconduct or other unanticipated circumstances by offering a framework that facilitates the identification of potential risks and the making of informed decisions.[4] It also makes Executive leaders answerable for the decisions they make, which results in increased organizational transparency.

[3] https://www.oecd.org/about/ visited on 7 March, 2024.
[4] R. Jain, "Impact of Cybersecurity Incidents on Corporate Reputation: A Case Study of Indian Companies," Journal of Business Ethics 35, no. 1 (2021): 205-220.

Corporate governance through the Board offers the essential supervision to ensure sustained financial success while defending stakeholder's investment interests. By putting good governance principles into practice, such as accountability, transparency, and goal-setting everyone is better equipped to recognize possible risks before they arise and take the appropriate precautions to avoid them. There is also more internal control when everyone knows their place in the system and what their responsibilities are. Additionally, it raises profit margins and enhances operational effectiveness. It is simpler for the partners to know how to react in the event of a problem, for instance, when an organization has a clearly defined set of responsibilities and expectations.

India has been growing digitally through technological development and there has been a drastic change in the way of businesses that are being done. There has also been a development in the interconnected business activities. In most cases, regardless of how secure a framework is, there is always a possibility that a better-equipped hacker is able to crack the code.[5]

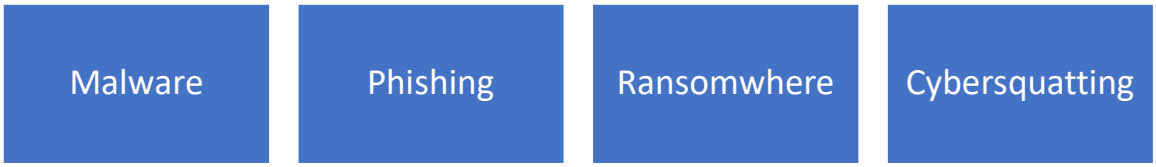
II. Cyber Security as an issue in Corporate Governance

Cybersecurity has grown into a complex and speeding security concerns in the age of information, communication and technology. Most financial and governmental institutions, military groups, corporations, hospitals and other businesses store; process huge amount of confidential information on computer and computer networks. The data passed to hackers, affect our lives in various ways which can lead to life-threatening situations. As a result, "cybersecurity" secures computer programmers, networks and secure information technology. [6] Cybersecurity also addresses preventing unauthorized individuals from retrieving information and preventing change or destruction. [7] Cybersecurity refers to a combination of tools, rules, regulations that can be applied to safeguard and secure cyber space.

Nowadays, information technology is used majorly in all business aspects as a key business enabler. Online software has been adopted by many big corporations for their works. This has made way to cyber risks. The hackers use the data stolen from large corporations to attain

[5] Simran Singh & Vaishnavee Upreti, Corporate Governance and Cyber Security, 4 INT'l J.L. MGMT. & HUMAN. 2808 (2021).
[6] OECD. (2012). "Cybersecurity Policy Making at a Turning Point. http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.
[7] Kearney, Rising to the challenge, http://www.kearney.com/web/global-business-policy-council/article?/a/rising-to-the -challenge_2018.

financial and monetary gains. Cyber hackers present themselves in various forms to attain monetary gains. Therefore, company faces a lot of cyber risks, the common risks faced are:



Malware – A form of cyber-attack in which harmful software's are installed into the computer systems without the user's awareness. This software can be introduced through various means such as through mails, software downloads etc.

Ransomware – This form of cyberattack where, once a link is activated, it scrambles the user's computer making it unavailable. The user has to pay huge sum of money to the hacker to unlock their systems. This is most hazardous type of cybercrime.

Cybersquatting – The hackers sells the victims domain name to the victim's competition in order to attain monetary benefits.

Phishing – A web page or email pops up that appears to be from an authentic source and the system gets hacked when the user clicks on the link. The main aim of the hacker is to extract personal information and sensitive data. In the case of National Association of Software and Service companies v. Ajay Sood[8], the concept of phishing was introduced in Indian law as the defendants were using the plaintiff's trademark "NASSCOM" to send spam mails and obtain personal information fraudulently.

Controlling and protecting cyber risk management is not a sole responsibility of the IT department. Thus, in the case of companies, cyber governance becomes a matter of the Board.[9] Policymakers are also held responsible for making insufficient laws and penalties so that effective measures can be taken by the board when a problem arises. The Indian government has recognized that there has been a drastic change in the increase of cyberattacks against financial and IT sectors. Spamming, email-bombing, cyber defamation cases have been reported all over the internet in India. India is ranked 88th globally in terms of internet connectivity, it is ranked 8th in terms of cyberattacks.[10]

[8] National Association of software and service companies v. Ajay Sood, 119 (2005) DLT 596
[9] Pricewaterhouse and Coopers, Turnaround and transformation in cyber security, 10 (2015)
[10] R. Kumar, "Cybersecurity Threats and Their Implications for Corporate Governance in India," Journal of Corporate Governance 15, no. 2 (2020): 45-67.

III. The Board's Role in Addressing Cyber Security Challenges

The role of the board of directors in addressing cybersecurity challenges is ultimate in today's digital landscape. With the increasing complexity of cyber issues, it is crucial for the board of directors to actively involve in cybersecurity governance and to protect the company's assets, reputation and its stakeholders.[11] The board should involve in setting clear policies and strategies, assessing risks, and monitoring the implementation of security actions. Board members need to understand the evolving nature of cyber threats and the potential impact on the organization's operations and financial health. Furthermore, the board should ensure that the company has a healthy cybersecurity framework in place, which includes immediate response plans, employee training programs, and regular security audits. By actively participating in cybersecurity discussions and decision-making processes, the board can demonstrate its commitment to protecting the company from cyber risks.

IV. Legal Frameworks for Cybersecurity in Corporate Governance in India

India has witnessed a significant rise in cybersecurity threats over the years, encouraging the government to establish a healthy regulatory framework to safeguard corporate governance practices. The regulatory landscape for cybersecurity in corporate governance in India is multi-layered and constantly evolving to address the dynamic nature of cyber threats.

The Information Technology Act, 2000

It serves as the cornerstone of cybersecurity regulations in India, providing legal recognition to electronic documents and promoting secure online transactions. Additionally, the Act empowers the government to prescribe guidelines for data protection and cybersecurity measures to be adopted by organizations. Section 43 of the act provides that "If any person accesses a computer, computer system or computer network without permission of the owner, or downloads, copies and extracts any data, or causes disruption of any system; inter alia, they will be liable to pay damages by way of compensation to the person so affected". This section covers the punishment for unauthorized access, ransomware, malware and all the attacks of a similar nature. Section 43[12] of the Act gives punishment for denial of service attacks.

[11] P. Sharma, "Role of Board of Directors in Cybersecurity Governance," Corporate Compliance Insights (2021), available at www.corporatecomplianceinsights.com.Companies Act, 2013, § 134, available at www.mca.gov.in.
[12] Information Technology Act, 2000, section 43(f): denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means.

Copyrights Act, 1957

Section 63 of the Copyrights Act talks about the electronic theft, which gives punishment for infringement of copyrights for a term which shall not be less than 6 months and which may extend to 3 years and with fine which shall not be less than Rs.50,000 but may be extended to Rs.2,00,000. Where infringement has not been made for gain in the course of business or trade, the court may impose sentence of imprisonment for a term less than 6 months or a fine less than Rs. 50,000.

Indian Penal Code, 1860

The Indian Penal Code also contains several sections related to cybercrime. Sections 379[13], 409[14], 419, 420 and 468 of Indian Penal Code which provides for punishment of theft, punishment of imprisonment and fine for criminal breach of trust by a public servant or an agent, punishment of cheating by personation and punishment of cheating respectively. Section 509 deals with offences relating to online stalking and harassment.

The National Cyber Security Policy, 2013

Cyberspace is a complex environment consisting between people, software and services, supported by worldwide distribution of information and communication technology devices and networks.[15] Information technology positively influences the lives of people through direct and indirect contribution to various socio-economic factors. The government has given key for increased adoption of IT based services. The National Cyber Security Policy serves as an umbrella framework for guiding the actions related to security of cyberspace. This policy therefore aims facilitate the cyber security framework, that leads to specific programmes and actions to enhance security in cyberspace.[16]

[13] Indian Penal Code Act,1860, Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
[14] Indian Penal Code Act, 1860, Whoever, being in any manner entrusted with property, or with any dominion over property in his capacity of a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

[15] https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf Visited on March 07, 2024.
[16] National Cyber Security Policy, 2013, available at www.meity.gov.in. visited on 07 March, 2024

Promotion of Research and development in cyber security to undertake research for addressing all aspects of development aimed at short, medium and long-term goals. By reducing the supply chain risks it is to build trusted relationships with employees for improving end-to-end supply chain. It was introduced to create a secure cyberspace ecosystem and enhance the resilience of national cyberspace. The policy lays down guidelines for the protection of critical information infrastructure, incident response, and capacity building in the cybersecurity domain.

The Reserve Bank of India (RBI) has issued cybersecurity guidelines for banks and financial institutions to mitigate cyber risks and ensure the integrity of financial transactions.[17] These guidelines encompass measures such as security operations centers, cybersecurity audits, and incident reporting mechanisms to boost the cybersecurity posture of the financial sector. Furthermore, the Securities and Exchange Board of India (SEBI) has mandated listed companies to disclose cybersecurity breaches and measures taken to mitigate cyber risks in their annual reports.[18] This regulatory requirement aims to enhance transparency and accountability in cybersecurity management among Indian companies.

Overall, the regulatory framework for cybersecurity in corporate governance in India underscores the importance of proactive risk management and compliance with cybersecurity standards to protect sensitive data and uphold the integrity of organizational operations. Adhering to these regulations it is imperative for Indian companies to navigate cybersecurity challenges effectively and foster a culture of cyber resilience in corporate governance practices.[19]

V. Practices for Enhancing Cybersecurity in Corporate Governance

Enhancing cybersecurity in corporate governance is authoritative in today's digital landscape where cyber threats are constantly evolving. Implementing best practices can significantly strengthen a company's defence against cyber-attacks and safeguard sensitive data. One of the fundamental best practices is to conduct regular cybersecurity risk assessments to

[17] Reserve Bank of India, "Guidelines on Cybersecurity for Banks," Circular No. RBI/2021-22/19, available at www.rbi.org.in. visited on 7 March, 2024.
[18] Securities and Exchange Board of India, "Cyber Security and Cyber Resilience Framework for Stock Brokers/Depository Participants," Circular No. SEBI/HO/MIRSD/DOP/CIR/P/2023/05, available at www.sebi.gov.in. visited on 7 March, 2024.
[19] M. Singh, "Regulatory Framework for Cybersecurity in India," Indian Journal of Corporate Law 25, no. 3 (2019): 112-135.

identify potential vulnerabilities and threats.[20]By understanding the organization's specific risks, companies can develop targeted strategies to mitigate these risks effectively.

Furthermore, implementing a vigorous cybersecurity framework that aligns with industry standards and regulations is crucial. This framework should encompass policies and procedures for data protection, access controls, incident response, and employee training to ensure a comprehensive security posture.

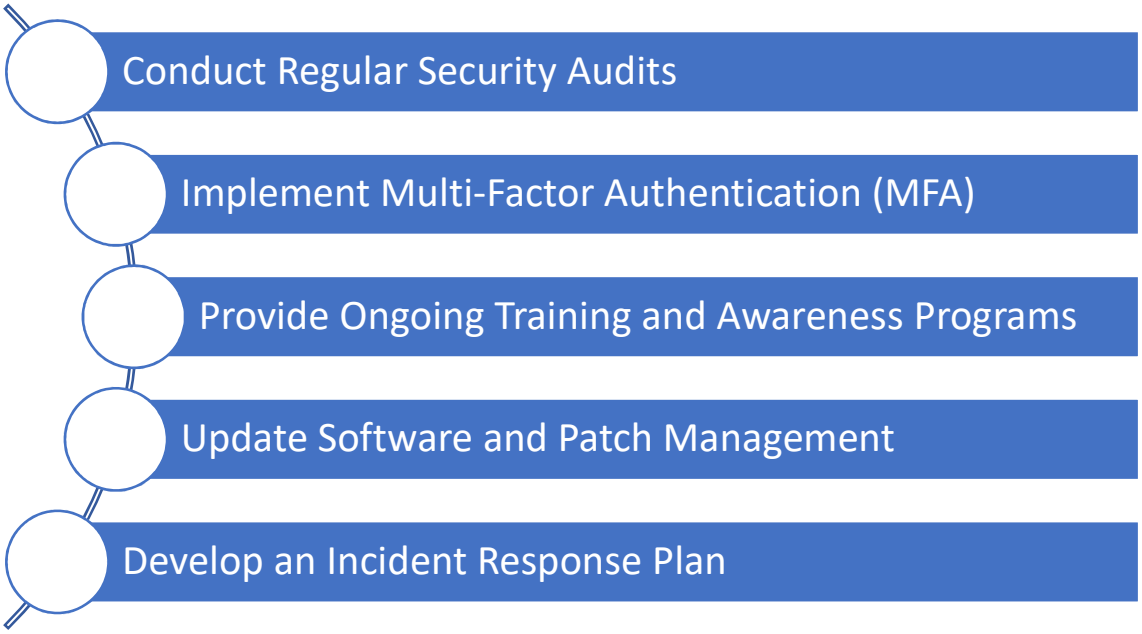
In addition, investing in advanced technologies such as endpoint detection and response (EDR), threat intelligence, and security analytics can enhance threat detection capabilities and enable proactive incident response.

Moreover, fostering a culture of cybersecurity awareness among employees through regular training and awareness programs is essential. Employees are often the first line of defence against cyber threats, and educating them about best practices for data security can significantly reduce the risk of human error leading to breaches.

By implementing these best practices and adopting a proactive approach to cybersecurity, Indian companies can effectively navigate the complex challenges of corporate governance and protect their critical assets from cyber threats.

Improving cybersecurity practices in Indian companies is crucial in today's digital age. To enhance cybersecurity measures and protect sensitive data, it is essential for organizations to implement robust strategies like:

[20] Indian Institute of Corporate Affairs, "Report on Cybersecurity Governance in Indian Companies," (2021), available at www.iica.gov.in.



Regular security audits help identify vulnerabilities and weaknesses in the existing cybersecurity framework. By conducting thorough audits, companies can proactively address potential risks and strengthen their defences. MFA adds an extra layer of security by requiring users to provide multiple forms of verification before accessing sensitive information. Implementing MFA can significantly reduce the risk of unauthorized access to company's data. Employee training and awareness programs are essential for promoting cybersecurity best practices within the organization. Educating employees about common cyber threats, phishing scams, and proper data handling procedures can help mitigate risks. Keeping software applications and systems up to date is crucial for addressing security vulnerabilities. Implementing a robust patch management strategy ensures that security patches are promptly applied to protect against known threats. In the event of a cybersecurity breach, having a well-defined incident response plan is critical for minimizing the impact and restoring normal operations quickly. Companies should outline clear procedures for responding to security incidents and designate responsible personnel to lead the response efforts.

By implementing these suggestions and adopting a proactive approach to cybersecurity, Indian companies can enhance their security posture and effectively mitigate cyber threats.[21] Prioritizing cybersecurity practices is essential for safeguarding sensitive data and maintaining the trust of customers and stakeholders in today's digital landscape.

[21] Ministry of Electronics and Information Technology, Government of India, "National Cybersecurity Strategy," (2019), available at www.meity.gov.in.

VI. Conclusion and Suggestions

It is evident that the landscape of cybersecurity is rapidly evolving, presenting both opportunities and threats to organizations. The digital transformation of businesses has brought about increased connectivity and efficiency, but it has also exposed vulnerabilities that can be exploited by cyber threats. Indian companies must prioritize cybersecurity as a critical aspect of their corporate governance framework. This involves fostering a culture of cybersecurity awareness and compliance at all levels of the organization, from the boardroom to individual employees. Regular training programs and simulated cyber-attack drills can help enhance preparedness and response capabilities.

Furthermore, investing in robust cybersecurity technologies and solutions is imperative to safeguard sensitive data and mitigate cyber risks. Collaboration with cybersecurity experts and information sharing platforms can provide valuable insights and best practices to enhance cyber resilience.

In addition, regulatory compliance with data protection laws and industry standards is essential to demonstrate commitment to cybersecurity governance. Regular audits and assessments can help identify gaps and areas for improvement, ensuring that cybersecurity measures are effective and up to date.

By adopting a proactive and holistic approach to cybersecurity governance, Indian companies can effectively navigate the challenges posed by cyber threats and protect their valued assets and reputation in an progressively digital world.[22] Embracing cybersecurity as a strategic priority will not only enhance trust and confidence among stakeholders but also drive sustainable business growth in the long term.

[22] Indian Institute of Corporate Affairs, "Report on Cybersecurity Governance in Indian Companies," (2021), available at www.iica.gov.in.