大成 DENTONS ACAS&LAW

The role of the Board in Cybersecurity and Information Technology (IT) Governance

Grow | Protect | Operate | Finance

February 2023

Introduction

Corporate governance encompasses the system of rules and regulations that governs the affairs of a company. It seeks to ensure that the financial and non-financial interests of all stakeholders in the corporate ecosystem are balanced.

It is important to highlight that Corporate Governance is based on three core principles which are accountability, transparency and security. For the purpose of this newsletter, our focus will be on security in relation to information technology as a principle in Corporate Governance.

Information Technology (IT) is a broad term that involves the use of technology to communicate, transfer data and process information. The different trends in information technology include but are not limited to analytics, automation, artificial intelligence and cybersecurity[1]. The world as we know it today is controlled by information as these forms the basis for some of our interactions, transactions, career and social network.

IT governance falls under security principles and is aimed at managing the usage of IT for the provision of value. As the world advances in its usage of IT across all sectors, it is imperative to ensure that laid out processes and guidelines are implemented to manage the usage of IT. The aim of IT governance is therefore to ensure that IT usage maintains the organizational objectives and policies and also create safety.

It has been established, particularly following the COVID-19 pandemic, that human interactions require technology for more effective communication. This is evidenced by the global social and professional population on communications applications such as Zoom, LinkedIn, Microsoft Teams and Slacks amongst others. It is therefore important to understand the need to protect the data exposures on these platforms.

Scope of Cybersecurity

The word cybersecurity emanates from two words, cyber and security. The Merriam-Webster dictionary[2] defines cyber to mean, of, relating to, or involving computers or computer networks (such as the Internet). Security on the other hand was defined to mean protection, that is, measures taken to guard against espionage or sabotage, crime, attack, or escape.[3]

1. What is Information Technology available at https://www.comptia.org/content/articles/what-is-information-technology#:~:text=Information%20technology%20is%20a%20broad,Artificial%20intelligence
2. "Cyber." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyber. Accessed 23 Jan. 2023.
3. "Security." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/security . Accessed 23 Jan. 2023

In merging the singular definitions of each term, what then is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access of criminal use and the practice of ensuring confidentiality, integrity, and availability of information.[4] Cybersecurity applies control mechanisms, thought-out processes and technologies, to manage significantly, the exposure and risks associated with cyberattacks. The collection and storage of our personal information, collection, financial and medical data has made it inherent for the development of cybersecurity mechanisms.

Types of Cybersecurity

Cybersecurity can exist in some of the underlisted ways:

1. ***Critical Infrastructure security*** – This includes all of the assets, systems and networks both physical and virtual, necessary for the effective functioning of a society's economy, national public health or safety, security, or any combination of the above.[5]
2. ***Application Security*** - Application security means a set of best practices, functions, and/or features added to an organization's software to help prevent and remediate threats from cyber attackers, data breaches, and other sources[6]
3. ***Network Security***- The network security consists of policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification or denial of a computer network-accessible resources.[7]
4. ***Cloud Security***- Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move towards their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.[8]
5. ***Internet of Things (IoT) Security*** - Internet of Things (IoT) security is the safeguards and protections for cloud-connected devices such as home automation, security cameras, and any other technology that connects directly to the cloud.[9]

Importance Of Cybersecurity to Corporate Organizations

Corporate organizations utilize data for measuring growth, developing business strategies, storing trade secrets, complying with regulatory updates and maintaining business sustainability amongst others. The security of this exposed data is a priority for any company's continued operations and sustainability. Therefore, the Board of Directors of a company should ensure that sustainable measures are implemented to uphold the necessary protection through IT Governance.

The IT Governance Institute[10] defines IT governance as an element of corporate governance, aimed at improving the overall management of IT and deriving improved value from investment in information and technology. It further states that an IT governance framework enables organizations to manage their IT risks effectively and ensure that the actions associated with information and technology are aligned with their overall business objectives.

4. Security Tip (ST04-001(What is Cybersecurity? Available at https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information.
5. What Is Critical Infrastructure? Why Does Critical Infrastructure Security Matter? -Available at https://www.paloaltonetworks.com/cyberpedia/what-is-critical-infrastructure
6. What is Application Security -Available at https://www.nutanix.com/info/what-is-application-security
7. What is Network Security- Available at *"What is Network Security? Poda myre". Forcepoint. 2018-08-09. Retrieved 2020-12-05.*
8. An Overview of Cloud Security- Available at - https://www.ibm.com/topics/cloud-security
9. What is IoT Security- Available at- https://www.proofpoint.com/us/threat-reference/iot-security
10. IT Governance: definition & explanation-Available at https://www.itgovernance.co.uk/it_governance

Implementation of IT Governance and the Role of the Board in Cybersecurity

Being a critical driver of strategic decisions that affect a corporate organization, the Board should be pro-active in setting out principles and developing strategies for upholding cybersecurity. This can be achieved by including IT governance strategy as an agenda item for discussion, given that most companies are equipped with advanced IT departments.

The Nigerian Code of Corporate Governance 2018[11] (the "Code") empowers the Board to provide oversight over Information Technology governance. The Code[12] recommends that the Board should establish a Risk Management Committee ("RMC" or the "Committee"). The Code further provides that the members of this committee should be responsible for risk management in an organization. Regarding the membership of the RMC, the Code recommends that the executive directors and the non-executive directors should be members of the Committee and the Committee should be chaired by a non-executive director.

The duties of the RMC are detailed in Part A, principle 11.5.6 of the Code. They include reviewing and recommending for approval of the Board, the risk management policies and framework, reviewing adequacy and effectiveness of risk management and controls, and exercising oversight over the process for the identification and assessment of risks across the company. It is noteworthy that one of the duties of the Board RMC is reviewing and recommending for approval by the board, at least annually, the company's information technology data governance framework to ensure that IT data risks are adequately mitigated, and relevant assets are managed effectively.

The framework may include[13]:

(i) Development of IT strategy and policy;

(ii) Proactive monitoring and management of cyber threats and attacks as well as adverse social media incidents;

(iii) Management of risks relating to third-party and outsourced IT service providers;

(iv) Assessment of value delivered to the Company through investments in IT; and

(v) Periodic independent assurance on the effectiveness of the Company's IT arrangements.

Without doubt, Nigerian law through the Code is pro-active in ensuring the security of data in corporate organizations. In addition to the above, the board should also ensure periodic external training for IT officers to ensure continuous education on how to forestall any breaches and maintain the security of data.

In developing the IT governance frameworks, the Committee and the Board must consider the underlisted as priority:

1. Ensuring a timeous decision-making process as it relates to IT governance.
2. Ensuring availability of regulatory support for compliance obligations and requirements.
3. Maintenance of a simplified and secured IT infrastructure.
4. Integration of the IT and risk management process for improved efficiency.

The Board must either by itself or through the Committee ensure the implementation of an effective IT governance framework.

11. Financial Reporting Council of Nigeria Act - The Nigerian Code of Corporate Governance (2018) Part A, Principle 1.10
12. The Nigerian Code of Corporate Governance (2018) - Part A, Principle 11.5
13. Section 11.5.6.6 The Nigerian Code of Corporate Governance (2018) - Part A, Principle 11.5 .6.6

IT GOVERNANCE – FRAMEWORKS AND MODELS

For the purpose of ensuring sustainable IT governance and seeking protection from cyber-attacks, some international standards have been established. The Board through the RMC or other special purpose committees is therefore encouraged to comply with these frameworks.

These international frameworks include:

a. ISO/IEC/38500:2015- being the international standard of IT corporate governance;

b. Information Technology Infrastructure Library (ITIL) being the framework for IT service management;

c. Control Objectives for Information Related Technology (COBIT)- an internationally recognized IT governance control framework that helps organizations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organizational goals and;

d. Calder-Moir IT Governance Framework, which provides structured guidance on how to approach IT.

Currently, the most recent technological innovation is the ChatGPT. ChatGPT is a very advanced smart technology that should be applied with care in any organization where the need arises. It is important that IT security be prioritized and embedded in the company's policy through its framework. The role of the Board of Directors, in this instance, will be to ensure that appropriate policies are established, applied and implemented to ensure safe management of data exposure.

CONCLUSION

In conclusion, the development of good IT governance cannot be overemphasized, particularly in terms of its benefits in protecting a business, its intellectual properties and digital assets from data breaches. As businesses continue to increase their reach through digital advancement with heavy reliance on technology, they must through its decision-makers, the board of directors, put measures in place to ensure protection from any IT breach or cyberattacks.

As established above, IT governance ensures that the business operations are protected from data and security exposure, particularly cyberattacks. It has been reported[14] that small and medium scale businesses have become increasingly exposed to cyberattacks. According to a report from Accenture's cost of Cybercrime study, it was reported that about 43% of cyberattacks are targeted at small businesses, the majority of which have not implemented structures to combat these attacks. This then leads to the winding down of these small businesses as a result of these attacks within 6 months of falling victim.[15]

Cybersecurity venture in its top cybersecurity predictions and statistics for 2023 predicted a 15% increased global cybercrime, and an expectation that over 6.5 billion people will use the internet[16] in 2030. This simply means a higher exposure for cyberattacks and cybercrimes. The Global cybercrime damage is predicted to hit $10.5 Trillion annually by 2025[17]

For context, the case of in LabCorp v. Metabolite, Inc[18] was a derivative suit brought against the company by one of its shareholders accusing the board of hiding the details of two data breaches that affected millions of patients. The shareholder claimed that LabCorp's " insufficient cybersecurity procedures" contributed a large part to the incidents.

One of the key takeaways from the LabCorp Suit is that all companies regardless of the size of their operations must invest in IT Governance. Investment in an IT Governance Framework is critical in ensuring that the company achieves overall success. It is therefore prudent for the board to oversee the development of IT frameworks to manage exposure to cybercrimes, cyberattacks, reputational damage, loss of personal data, intellectual property theft, loss of funds, and embezzlement amongst others.

14. 2023 Must-Know Cyber Attack Statistics and Trends- Available at https://www.embroker.com/blog/cyber-attack-statistics/ https://cybersecurityventures.com/research/
15. Cybersecurity Research: All in One Place- Available at https://cybersecurityventures.com/research/
16. Cybersecurity Research: All In One Place- Available at https://cybersecurityventures.com/research/
17. Top 10 Cybersecurity Predictions And Statistics For 2023- Available at https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/
18. LabCorp slapped with shareholder suit over data breaches Available at - https://techcrunch.com/2020/04/30/labcorp-suit-data-breaches/?guccounter=1

ABOUT DENTONS

Dentons is designed to be different. As the world's largest global law firm with 21,000 professionals in over 200 locations in more than 80 countries, we can help you grow, protect, operate and finance your business. Our polycentric and purpose-driven approach, together with our commitment to inclusion, diversity, equity and ESG, ensures we challenge the status quo to stay focused on what matters most to you.

www.dentons.com

CSBrand-109535-Article - The role of the Board in Cybersecurity and IT Governance-02 — 09/02/2023