International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security Governance

Mohammed Mustafa Khan

Abstract
The massive coordinated cyber-attack that struck Estonia in April 2007 and lasted for many days is a remarkable incident that explains the significance of cyber security governance for any institution that has embraced the digital world economy. No institutions would want such attacks to disrupt and dominate their operations since it has devastating effects. The cyber threat landscape is ever-evolving in that new tricks of attacks are being launched daily. It takes an institution to develop a comprehensive cybersecurity governance to keep pace with emerging trends. Institutions that have failed to deploy cyber security governance succumb to different types of cyber threats. The one non-negotiable aspect that institutions must not ignore to employ is cyber security governance. Cyber security governance helps organizations to minimize cyber security breach incidences. This research paper explores the importance of implementing effective cybersecurity governance strategies, emphasizing the need for alignment between cybersecurity policies and overall business objectives.

Keywords: cybersecurity Governance, Cyber Threats, business objectives, IT Infrastructure,

1.0 Introduction

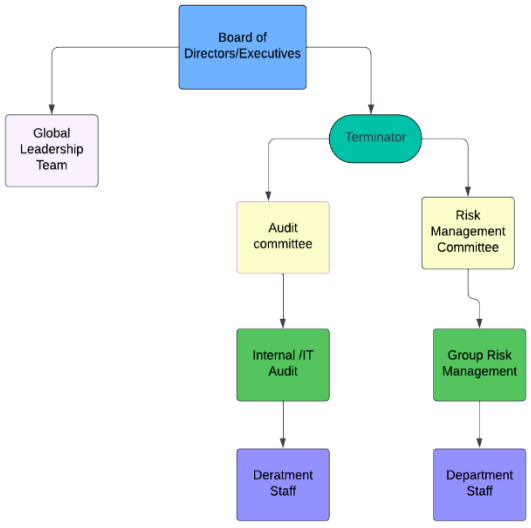
Cybercriminals have become relentless in executing attacks on organizations. Any organization is susceptible to attack. The question that is difficult for the security operation team to answer is when the attack is happening. Attacks are pervasive in nature, so it is a tremendous aspect to plan adequately before they are exploited. Over the years, the executive teams debunked cyber security and focused only on the business processes and objectives to maximize their competitive advantage. It did not go well with organizations that ignored cyber security governance. Their operations were disrupted, leading to downtime, loss of revenue, and reputational damage. For instance, Telefonica, a Spanish telecommunication company, had its IT systems attacked by WannaCry ransomware, which infested the internal server and led to lateral spread to the employee workstations [9]. This scenario demonstrates the importance of having a solid cyber security governance that can act as the first line of defense against modern threats. The board of directors, IT personnel, employees, and all the stakeholders should work in tandem to ensure the cyber security culture is inculcated through the establishment of a comprehensive cyber security governance. Cybersecurity governance has become part and parcel of organizational strategy. This paper discusses an overview of cybersecurity governance, examining how it aligns with corporate governance and risk management practices. Organizations can secure their assets, protect sensitive information, and ensure compliance with regulatory requirements by understanding and implementing strong cybersecurity governance. Additionally, the paper also delves into the challenges organizations face during the implementation and offers strategic solutions for overcoming them.

2.0 Overview of Cybersecurity Governance

2.1 Understanding Cyber Security Governance

Cyber security governance is the act of defining, administering, and implementing protocols, policies,

guidelines, frameworks, and controls to protect the IT infrastructure against cyber risks. It involves how cyber security practices are enforced and coordinated in an institution [10]. It trickles down to having an understanding of the structure of responsibilities and accountability that entails carrying out what decisions are required to be made, who is supposed to make such decisions and the personnel that is supposed to keep the structures in check. Audits are crucial in cyber security governance since they validate whether the approach taken for cyber security is meeting its objectives. An effective and efficient cyber security governance framework is one that functions properly and includes all the stakeholders in an organization. It should operate in such a way that individuals in an organization are able to properly manage risks within their related level of responsibility. Security governance focuses on the top management leaders, and it drills down to their subordinate staff and relevant stakeholders to ensure awareness is raised. Establishing a comprehensive cyber security governance enables employees to fathom their roles and responsibilities pertaining to organizational cyber security. The top management level should not delegate the cyber security best practices only to the IT and security teams. However, they should incorporate cyber security governance as the organizational strategic resource that must be implemented to ensure that the organization attains its vision without disruptions from cyber threats [10]. Cybersecurity governance differs from one organization to another. It is important for every organization to assess its vulnerabilities and establish its own cyber security governance program. The following diagram shows an example of a cyber security governance organogram.



2.2 The goal of Cyber Security Governance

The objective of cyber security governance is to ensure confidentiality, integrity, and availability of resources and information and that enterprise IT assets are utilized appropriately [6]. Cyber security governance must provide a structured approach to manage and mitigate cyber security risks in an organization. Effective cybersecurity governance must be an integral and transparent component of an institution's governance. With a drive towards efficiency in production through automation, today's organizations rely on digital technology to support business processes and operations. It is crucial to ensure the data th't resides in the servers and computers is confidential, not altered or damaged, and i' available any time a legitimate user accesses the data. Cybersecurity governance ensures proper implementation of security programs to ensure the confidentiality, integrity, and availability of resources and information [6]. Additionally, cyber security governance demonstrates the diligence and concern that organizations

have taken to protect their IT assets against sophisticated attack vectors. The governance works to ensure policy and regulatory compliance are met, and potential cyber risks are properly addressed to minimize penalties and repercussions in the event of security breaches. Effective governance ensures the alignment of cyber security with business goals and objectives. This strategic alignment creates a business culture and structure that drives the security requirements, which ensures the organizations achieve their objectives.

3.0 Components of Cyber Security Governance (CSG)

3.1 Risk management

Risk management in cyber security governance entails discovering, assessing, and ensuring prioritization of risks that could damage an organization's IT infrastructure. Additionally, risk management can be used as a tool to detect and disrupt risks. After discovering the risks, the preliminary step that takes the stage is an assessment to determine their possible effects and probability of happening [1]. The goal of this process is to allow an organization to evaluate how they should allocate resources to combat the risks depending on the criticality and severity. During the development of a cyber security governance strategy, it is imperative to factor out risk management and align it with business objectives. This will ensure proper risk mitigation and business continuity in the event of cyber security disasters. Organizations must ensure risk management is a proactive and continuous process since cyberattacks are a non-stop activity.

3.2 Compliance

Compliance ensures an organization's cyber security programs conform to regulatory requirements. Regulatory compliance ensures data security, protects critical data from unauthorized access/usage, and upholds business ethical practices. Organizations use many regulatory requirements depending on the nature of their business activities [1]. Healthcare sector businesses are supposed to ensure the safety of patient data from unscrupulous users by ensuring they abide by the HIPAA (Health Insurance Portability and Accountability Act) regulatory requirements. Businesses that deal with online payment transactions must ensure they adhere to the PCI DSS (Payment Card Industry Data Security Standard) Act to minimize payment card fraud by optimizing security controls around the cardholder data. Businesses that operate around the European unions must maximize the use of GDPR (General Data Protection Regulation), which is a regulatory requirement enforced on all the European member states that governs the collection and processing of personal information from individuals. There are several regulatory laws, such as CCPA

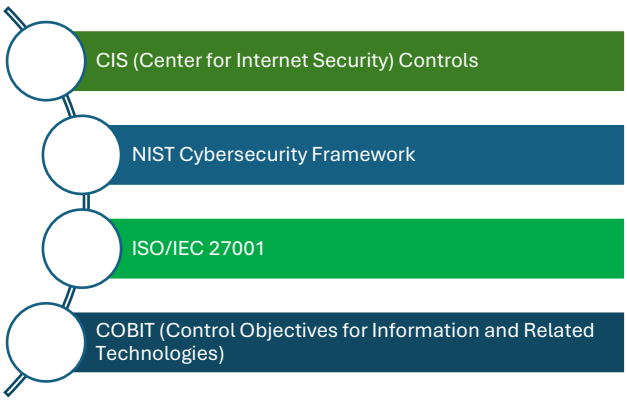
(California Consumer Privacy Act), that ensure data privacy, business ethics, and processing of individual data of California residents is performed in accordance with the law. Cybersecurity governance must feature all these standards in its strategy depending on the federal laws of the land. Implementing these standards demonstrates the efforts and transparency in the eyes of partners, customers, and all the stakeholders.

3.3 Incident Response

Incident response is the backbone of cyber security governance. It is an accepted truth that no member of the board of directors can welcome temporary shutdown or premature termination of their business activities due to cyber threats. It is vital to develop and implement recovery plans to manage and remediate the effects of cyber security threats [1]. Cyber security governance should focus on investing in advanced detection and response tools to ensure systems and networks are monitored and any signals of malicious or unusual activities are detected and disrupted instantly. Once the incident breach is detected and disrupted, investigation and remediation plans must be implemented to prevent future occurrences of similar incidents. After resolving the incidents, recovery plans are executed by restoring the systems to their normal operations to ensure business continuity. Organizations that fail to incorporate incidence response in their cyber security governance may find it difficult and take several longer days to restore their businesses to normalcy.

4.0 Frameworks for Cybersecurity Governance

Frameworks are the premier foundation of cyber security governance. They are the building blocks that support a structured approach to developing a cyber security governance program. There are several frameworks that exist that can help corporate governance to develop a comprehensive program. These frameworks can be amalgamated or used individually to enhance the creation of cyber security governance. Integrating all the frameworks during the development ensures that a superior cyber security governance strategy is adopted. Here are some of the lists of frameworks that can be used.



4.1 The CIS Controls

The CIS controls provide a more practical, actionable set of cyber best practices to shield IT infrastructure against attacks. The controls are classified into three categories: basic, foundational, and organizational [5]. Additionally, CIS Controls offer implementation groups to aid organizations in prioritizing their

efforts depending on the level of resources and risk severity. The v8 of CIS Controls provides 18 controls and 153 safeguards to help organizations develop an effective cyber security governance.

4.2 The NIST Cyber Security Framework (CSF)

It was developed by the National Institute of Standards and Technology to help organizations protect organizations against cyber threats. This framework can be incorporated into the Cyber security governance strategy since it centers around five core functionalities, including Identify, Protect, Detect, Respond, and Recover [2]. Organizations can associate these five core functions to meet their overall goals of cyber security governance. Additionally, there are implementation tiers that the NIST CSF provides to aid organizations in accessing and evaluating their strengths and weaknesses of cyber security practices and spot areas for improvement.

4.3 ISO/IEC 27001

ISO/IEC 27001 is a standard that focuses on information security management systems. The standard provides a step-by-step approach to managing sensitive company information. It addresses risk assessment and remediation by indicating various best practices for information security [3]. This standard can not be left out when developing cybersecurity governance. It provides guidance on how the security controls must be implemented. Corporate governance can leverage the use of this standard to ensure that cyber security governance is effective and efficient.

4.4 COBIT framework

The COBIT framework was developed by ISACA to synergize technical issues and control requirements and business risks. COBIT focuses on the alignment of information technology with business goals; thus, it helps in the provision of governance and management objectives [4]. This framework is a handy tool for organizations that want to optimize the integration of IT governance with corporate governance. Its implementation extends to cyber security since it outlines how IT leaders should instill a culture of cyber security to the other non-IT staff.

5.0 Best Practices for Implementing Cyber Security Governance

5.1 Developing a Comprehensive Cyber Security Plan

The cyber security strategy must correspond to business and IT objectives. Policies and best practices must be developed by top leaders, such as chief information security officers (CISOs). It is essential for the CISO to engage with various entities such as cybersecurity professionals, heads of departments, employees, and all the stakeholders to ensure no cyber threats are left unturned, and all the areas are covered in the program. The approach can entail risk management and assessment to discover, assess, and remediate possible threats to the company's systems and data [1]. Implementing role-based access controls to ensure audits can be easily conducted in case of data breach incidents and establishing incident response protocols are essential aspects of the strategy since they will provide actions to be taken in the event of a cyber catastrophe.

5.2 Maximizing Advocacy Programs

The governance develops policies and assigns them to various employees. Each member has a role to play in ensuring the established policy security standards are followed strictly [1]. However, the leadership

must not develop these policies and just mount them on walls where employees can view them as they progress to their workstations. The leadership must go beyond mounting security policies on walls and sensitize all the stakeholders on the importance of adhering to security policy standards. They can develop training programs and conduct workshops and webinars to create awareness among all the employees and stakeholders of the organization. Provide adequate training to employees on matters pertaining to social engineering attacks, ransomware, and password policy best practices, among others. Training and education programs must be a continuous process since the cyber threat landscape is emerging, and employees must be kept updated with these modern threats [1].

5.3 Monitoring and Evaluating

Continuous monitoring and evaluation of cyber security governance is crucial when upholding cyber resilience. Cybersecurity governance must create a policy that covers the constant monitoring and investigation of network activities that detect and disrupt them to enable instant responses to potential threats before escalating into security breaches [1]. Corporate governance can employ cyber threat-hunting tools that have threat intelligence capabilities that can help organizations keep abreast of cyber criminals. It is important to validate if the deployed security tools function per their intended purposes by evaluating them through rigorous testing programs. Vulnerability assessment and penetration testing should be regularly conducted to ensure no weak points that can be exploited by cybercriminals.

5.4 Agility and Adaptability

Organizations must be flexible enough to properly tackle the ever-emerging threat landscape. The IT and security teams may spot an important loophole in a particular security policy and recommend changes. However, their efforts to fix the issue in time have to wait for a long time due to the bureaucratic nature of decision-making among executives. Leadership ought to determine the ways of collectively investigating and implementing the suggested changes before things get out of their hands. Leadership must be willing to relook and review such recommendations and swiftly implement the changes.

6.0 Challenges in Implementing Cyber Security Governance

6.1 Resource constraints

Some organizations have limited budgets and resources for the implementation of a comprehensive cybersecurity governance program. Additionally, an effective program may require investing in advanced cybersecurity tools and solutions, which are very expensive for some organizations [8]. Organizations can start small by properly allocating the budget and the resources to avoid the grave effects of cyber threats.

6.2 The ever-changing threat landscape

Advanced modern threats can evade the underlying security controls that end up compromising critical company information. Implementing the basic level of cyber security governance cannot remediate these modern threats [8]. Organizations need to implement advanced threat detection solutions that can protect the IT infrastructure.

7.0 Conclusion

Cybersecurity governance is a crucial element of any cybersecurity program. It dictates how an organization is ready to deal with the emerging threats. It is crucial for organizations to develop or modify

the cyber security governance to align with the business objectives. Effective cyber security governance will foster businesses in achieving their vision since it eliminates or minimizes cyber security incidents and also ensures organizations meet various regulatory compliance requirements. By reducing or eliminating data breaches and meeting regulatory requirements, organizations build their reputation and create a level of trust in clients and customers, avoid penalties in terms of fines imposed by failing to implement regulatory standards, and increase revenue. The directors, executive management, and IT leaders should comprehend the elements of cyber security governance, the frameworks that will enable its development, best practices to implement, and challenges that they can incur to ensure they establish or modify the cyber security governance program that covers people, process, and IT infrastructure. Top management should ensure that the organization is properly structured and managed with powerful policies and a strong ethos. Good governance breeds a culture which is strictly followed and anyone who breaks the rules must be held accountable and treated in accordance with what is indicated in the policy document.

8.0 Reference:

1. DataGuard, “Cyber Security Governance - Policies, Processes & Controls for Businesses,” *Dataguard.co.uk*, Jul. 2018. https://www.dataguard.co.uk/cyber-security/governance/
2. A. Calder, "NIST Cybersecurity Framework: A pocket guide," *Google Books*, Sep. 2018. https://books.google.com/books?hl=en&lr=&id=rWxvDwAAQBAJ&oi=fnd&pg=PT9&dq=+NIST+Cybersecurity+Framework&ots=q_i23UCmwn&sig=QatbSxOVf6Bihfe37QvivhYAkDc
3. H. Edward, "Implementing the ISO/IEC 27001:2013 ISMS Standard," *Google Books*, Mar. 2016. https://books.google.com/books?hl=en&lr=&id=Yy6pCwAAQBAJ&oi=fnd&pg=PR6&dq=ISO/IEC+27001+Cybersecurity+Framework&ots=vss16kg7YQ&sig=uq0XnjnxMmBxR43D_5EvA7WO5ms
4. S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, "COBIT as a Framework for Enterprise Governance of IT," *Management for Professionals*, pp. 125–162, Sep. 2019, doi: https://doi.org/10.1007/978-3-030-25918-1_5.
5. Center for Internet Security , "CIS Controls v8," CIS, May 18, 2021. https://www.cisecurity.org/insights/white-papers/cis-controls-v8
6. The Federal Virtual Training Environment, "Cybersecurity Governance," Nov. 2020. Available: https://fedvte.usalearning.gov/publiccourses/FCSM/course/videos/pdf/FCSM_D01_S03_STEP.pdf
7. Defense Cybersecurity, "Cybersecurity Governance – Defense Cybersecurity," *Dcybersecurity.sa*, Feb. 2021. https://dcybersecurity.sa/cybersecurity-governance-practices/
8. S. Swinton and S. Hedges, "Cybersecurity Governance, Part 1: 5 Fundamental Challenges," *SEI Blog*, Jul. 25, 2019. https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/
9. C. Alejandro, T. Guarda, and G. Ninahualpa Quiña, "Ransomware - WannaCry Security is everyone's," *ieeexplore.ieee.org*, Jun. 19, 2019. https://ieeexplore.ieee.org/abstract/document/8760749/
10. E. Ryan and V. Mohan, "Rewired," *Google Books*, Apr. 24, 2019. https://books.google.com/books?hl=en&lr=&id=xmONDwAAQBAJ&oi=fnd&pg=PA11&dq=Components+of+Cyber+Security+Governance&ots=TYlUeNlC_S&sig=8oqVtGoJLySU_fPbCNpcMu6G6-I