Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 9, No 4, December. 2023 Series

The Role of Frameworks in Cybersecurity Governance

[1]Jimoh, H.O., [2]Fagade, M.O. & [3]Ahmed, M.O.
[1, 2] Department of Cybersecurity
The Federal Polytechnic, Offa, Kwara State.
[3] Cisco Systems, Nigeria
Lagos, Nigeria
E-mails: [1]hamid.jimoh@gmail.com, [2]fagad.ola@gmail.com & [3]mublamouchi@gmail.com

ABSTRACT

With the present digital world, we are in today, cybersecurity has become more pervasive for companies, government agencies, organizations, and the end-users. However, since digital data in cyber environments is also rapid, security measures have gained more importance. National and international units reveal cybersecurity threats, and this number of threats is increasing daily. The elimination of cybersecurity risks is possible with an effective cybersecurity strategy. Since the concept of management is insufficient, implementing this strategy is possible with cyber governance, which includes all stakeholders in the management processes. This paper emphasizes the role of frameworks in cybersecurity governance, which discusses some of the management tools required for decision-making, a comprehensive risk management approach, and, most importantly, an organization-wide security awareness program. We will compare different frameworks from IT governance to cybersecurity and the advice on the best-fit framework for an organization to achieve its desired objectives.

Keywords – Cybersecurity, Framework, IT Governance

Journal Reference Format:
Jimoh, H.O., Fagade, M.O. & Ahmed, M.O. (2023): The Role of Frameworks in Cybersecurity Governance
Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 9. No. 4, Pp 7-16.
Available online at https://www.isteams.net/behavioralinformaticsjournal. dx.doi.org/10.22624/AIMS/BHI/V9N4P2

1. INTRODUCTION

Information technology has proliferated over the years. The acceptance of computers in most aspects of our lives from business, government, education, finance, health, transportation, etc., has also increased lately. With this acceptability, the consequences of cybercrime can be catastrophic if there are no effective policies and measures taken. Organizations regardless of their size and purpose, accept and store data and information on the computer system, some of this data and information are crucial to organizational development. However, this data and information has to be transmitted either from one device to another or via the internet.

During this transmission process, data and information can be subjected to being hijacked or compromised. Also, Due to the new technologies coming up daily, the threat of information security from criminals, terrorists, and hackers has increased which can lead to serious Information Technology or Data breach. Hence a need to develop a strategic framework to secure business organizations and entities. Information Technology or Data breaches have affected several organizational systems in various countries across the globe; some of which are critical infrastructural systems like health, education, Tech industries, etc.

Security breaches and computer viruses cost global businesses $1.6 trillion a year and 39,363 human years of productivity. In 2009, Symantec detected 59,526 phishing hosts around the globe, that number is increased by 7 percent compared to phishing hosts detected in 2008. The percentage of threats to confidential information has increased to 98 percent in 2009 compared to 83 percent in 2008. 89 percent of the threats can export user data and 86 percent of them have keystroke-logging components" [1]. This is a serious concern as there is every possibility that the percentage may increase to 90 or 95 percent in 2022.

Like the rest of the world, Africa has its share of cyber-attacks; some of which are ransomware, Botnet, online scams via phishing, digital extortion, etc. In 2021, data has shown that South Africa is the most targeted, followed by Kenya, Nigeria, and Ethiopia. However, "Nigeria and Ethiopia have had the highest increase of cyber-attacks on the continent compared to the pre-covid year. Nigeria, Ethiopia, and South Africa recorded an increase of 23 percent, 20 percent, and 14 percent, respectively, with Kenya being the only country that saw a decrease of 13 percent. Nigeria seems to be the most hit. Yet, experts see more attacks on businesses as the migration towards Internet-of-Things (IoT), Artificial Intelligence, and cloud computing continues to grow while exposing them to cyber-attacks risks" [2]

Today, the prevalent attacks in cyberspace are drastically increasing daily which could be due to a lack of security assistance, system vulnerabilities, limited or no security awareness, lack of risk assessment, etc. For this reason, the role of cybersecurity governance framework has emerged which gives directions and guidance to business organizations on how to implement proper cybersecurity policies, sensitization of cybersecurity programs at all levels, ensuring continuous assessment of risk, etc. Although the organizational structure of management and governance processes differs, the key objective is that when there is a proactive information security practice and application of governance principles and practices at every level of the organizational hierarchy, this will reduce cybersecurity risk and greatness can be achieved in the organization

This paper aims to discuss extensively the concepts of cybersecurity, governance, and framework and how pertinent IT governance framework along with cybersecurity framework and cybersecurity governance framework are in an organization.

Cybersecurity

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security [3]. Basically, with this definition, cybersecurity can be summarized as the protection of cyber systems against cyber threats.

Concept of Governance

Governance can be defined as "The system by which entities are directed and controlled. It is concerned with structure and processes for decision-making, accountability, control, and behavior at the top of an entity. It also influences how an organization's objectives are set and achieved, how risk is monitored and addressed, and how performance is optimized" [4].

Concept of Framework

A framework is generally described as the abstract, logical structure for organizing information that will guide the development of a study. The definitions and understanding of frameworks range from different perspectives; legal, organization, business, etc. From the legal perspective, a framework can be defined as "a system of rules, ideas, or beliefs that are used to plan or decide something. However, from an organizational point of view, a framework can be defined as "the idea, information, and principles that form the structure of an organization or plan. In business, a framework can be defined "as a system of rules, ideas, or beliefs that are used to plan or decide something" [5]. The act of establishing and using a framework is to solve to solve economic problems. It will be observed that the definition of a framework for business and organization is relatively the same.

Definition of IT Governance

IT governance "is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives" [6].

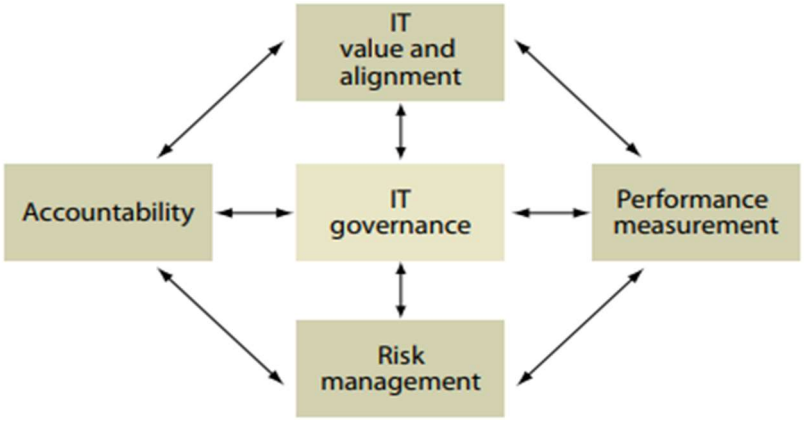

Figure 1: The Four Dimensions of IT Governance [12]

The diagram above summarizes the four objectives of IT Governance and each of the objectives (IT value & alignment, accountability, risk management, and performance measurement) must be addressed as a component of the IT governance process.

2. IT GOVERNANCE FRAMEWORK

IT Governance framework is a roadmap that defines the ways and methods used by an organization to implement, monitor, and manage IT governance within the organization. In other words, the use of frameworks can help greatly to improve governance, structure, and clarity in areas such as enterprise architecture, service management, and enterprise architecture.
Implementing good IT governance requires a framework that is based on 3 key elements; Structure, Process, and Communication. [7]

- Structure: Who makes the decisions? What structural organizations will be created, who will take part in these organizations, and what responsibilities will they assume?
- Process: How are IT investment decisions made? What are the decision-making processes for proposing investments, reviewing investments, approving investments, and prioritizing investments?
- Communication: How will the results of these processes and decisions be monitored, measured, and communicated? What mechanisms will be used to communicate IT investment decisions to the board of directors, executive management, business management, IT management, employees, and shareholders?

While there's no specific or complete IT governance framework, there are a few that are useful for the development of a governance model. In this paper, we will be discussing a few of the widely used frameworks such as COBIT, ITIL, NIST CSF, ISO/IEC 27001, etc. Each of the listed frameworks has its significant IT governance strengths.

COBIT

Control Objectives for Information and Related Technology (COBIT) was developed in 1996 by The Information Systems Audit and Control Association (ISACA) which is presently issued and maintained by the IT Governance Institute (ITGI) as a framework to provide management and business process owners with an IT governance model to help understand and manage the risks associated with information technology. Although, according to the third COBIT edition, it has been extended to serve as an IT governance framework by providing maturity models, critical success factors, Key Goal Indicators (KGI), and Key Performance Indicators (KPI) for the management of IT. However, at the heart of COBIT, are 34 high levels, they consist of four main components which include planning and organizing, acquisition and implementation, delivery and support, and finally, Monitoring and evaluation [8]. Basically, In the implementation of IT governance, COBIT represents a comprehensive framework for implementing IT governance with a very strong auditing and controls perspective which in turn improves the security and quality of production of the organization.

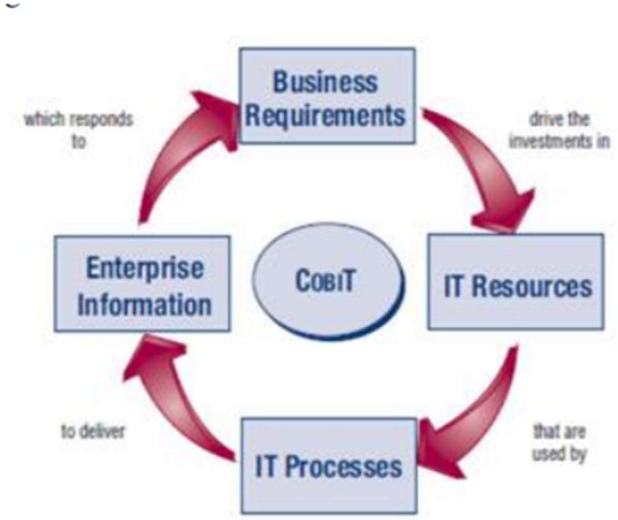

Figure 2: COBIT Framework [13]

ITIL

ITIL The information technology infrastructure library (ITIL), is the most widely used approach in managing IT services. It was initially developed in the UK by the Office of Government Commerce (OGC), as a library of best-practice processes for IT Service Management. ITIL is now becoming popular and widely accepted globally in the IT community as a framework for IT governance and it's supported by ISO/IEC 20000:2011, against which independent certification can be achieved. While COBIT takes the perspective of audit and control, ITIL takes the perspective of service management.

The two frameworks are more complementary than competitive and components of both can be taken to build a governance framework. The library currently consists of eight books, including: "Software Asset Management," "Service Support," "Service Delivery," "Security Management," "Application Management," "ICT Infrastructure Management," "The Business Perspective," and "Planning to Implement Service Management". ITIL assists organizations in delivering their services in a customer-focused, economical, and quality-driven way.

ITIL has different versions that range from V2, V3 to V4. The ITIL Version 2 was released in 2000/2001 and consists of two publications (Service support and Service delivery). Also, the ITIL Version 3 and service lifecycle was released in 2007 with 5 publications (Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement). The ITIL Version 4 was given the holistic approach and it's the most recent. It supports organizations that adopt digital transformation by integrating digital technology into most of the areas of their business.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 9, No 4, December. 2023 Series

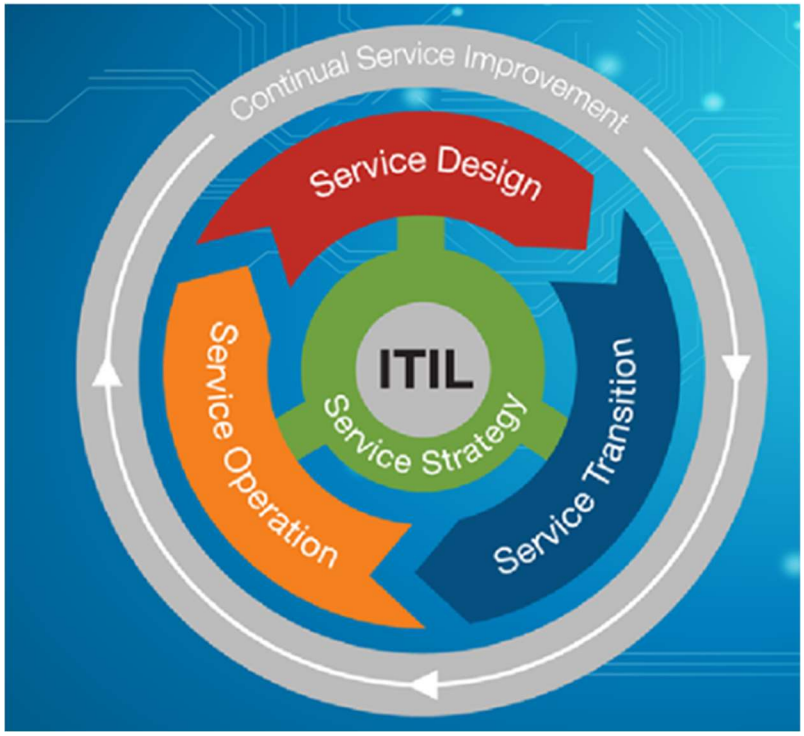

Figure 3: ITIL (Information Technology Infrastructure Library) [14]

3. CYBERSECURITY FRAMEWORKS

ISO/IEC 27001

With the significant increase in information technology, organizations face tougher pressure to secure their internal and external information. Therefore, there is a need for urgent adequate measures for information security. Presently, the number of security breaches is increasing, and adversaries and getting smarter in their ways to exploit security vulnerabilities. Hence a need to develop a security framework to manage the confidentiality, integrity, and availability of information assets. ISO/IEC 27001 standard has been developed for protecting organizations' information assets and was published in 2005 under the Information Security Management Systems (ISMS).

The Information Security Management System (ISMS) as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 is an international standard with an overall program that combines risk management, security management, governance, and compliance. It also assists in providing requirements for establishing, implementing, maintaining, and continually improving information security practices in organizations. "ISO/IEC 27001 is an integrated part of the organizations' processes and overall management structure and information security is considered in the design of processes, information systems, and controls.

The standard applies to all organizations, regardless of their type, size, or nature and it constitutes a certifiable standard and is widely used with steady growth in several adoptions" [9]. As more and more information is digitally created, processed, and stored, and more percentage of companies' revenue is generated by information-critical processes, the more valuable an asset ISO/IEC 27001 standard becomes. "One of the benefits of this framework is that it helps most organizations to ensure that the right people, processes, and technologies are in place, and facilitates a proactive approach to managing security and risk" [10]. To authenticate the compliance of ISMS with ISO 27001, an organization has to pass a certification procedure controlled by an authorized certification organization called Registered Certification Bodies (RCB). This certificate is valid for 3 years, after that, a re-certification can be applied for.

NIST CSF

Another important cybersecurity framework is the NIST CSF (The National Institute of Standards and Technology Cybersecurity Framework). This framework explicitly gives a detailed guide to organizations to improve their understanding of managing, reducing, and communicating cybersecurity risks. In cybersecurity, it is crucial to understand how to manage the risk by organizing the information, enabling risk management decisions, addressing threats, and learning from previous activities. NIST CSF is essential and the foundational resource used by most sectors around the world. The sectors include critical infrastructure systems; such as the health system, transportation system, Energy grid, manufacturing system, etc. For these systems, it is pertinent to understand the basic cybersecurity threat activities at their highest level. Reports and reviews have it that NIST CSF has maintained its effectiveness in addressing cybersecurity risks by coming up with programs to address governance and risk management and enhancing communication within and across organizations.

Despite the enhancement, CSF is still subject to be refined and improved upon over time. "NIST initially produced the Framework in 2014 and updated it in 2018 with CSF 1.1. The CSF is being updated openly with input from government, academia, and industry, including through workshops, public review and comment, and other forms of engagement. With this update, NIST is open to making more substantial changes than in the previous update. The "CSF 2.0" version reflects the evolving cybersecurity landscape— but community needs will drive the extent and content of the changes" [11]. Cybersecurity framework is classified into functions such as identity, protect, detect, respond, and recover. Each of these functions has their respective categories

Figure 4: NIST Cybersecurity Framework [15]

3.1 Cybersecurity Governance Framework

ISO/IEC 27014

One of the key cybersecurity governance frameworks is ISO/IEC 27014. Generally, the International Organization of Standardization (ISO) is a global federation of national standards bodies and this body collaborates closely with the International Electrotechnical Commission (IEC) on matters concerning electrotechnical standardization. In 2013, ISO/IEC published an international standard for the governance of Cybersecurity as ISO/IEC 27014, part of the 27000 series of standards that will help organizations secure their information assets.

The standard includes guidance on the concepts of ISG of aligning IS activities with organizational strategy, based on six high-level principles. The principles are the accepted rules for governance actions. The standard specifies five governance processes: evaluate, direct, monitor, communicate, and assure, which need to be implemented by the governing body and executives These principles enable the organization to establish a wide information security that adopts a risk-based approach to set the direction of investment decisions. It also ensures conformance with the internal and external requirements to foster a positive security environment.

4. ROLE OF FRAMEWORKS IN CYBERSECURITY GOVERNANCE

The need for effective governance cannot be overemphasized. The reason why most organizations; both public and private sectors, must incorporate good governance practices and principles into their daily business activities to achieve their organizational goal and objectives. The governance principles and practice are exercised by those responsible for an enterprise (e.g., the board and executive management, the head of a federal agency); to provide strategic direction, and ensure that objectives are achieved. CGF includes guidance for developing comprehensive strategies that assist the organizations in coming up with a business continuity plan.

As such, adds to the establishment of metrics used in measuring success. The cybersecurity governance framework has several processes. Some of these include; Cyber Risk Assessment, Business Impact Analysis, Cybersecurity Strategy Development, Governance Committee, and Cybersecurity Policy and Procedures. In summary, CGF helps with compliance and risk management and ensures everyone is doing their job and that the organization adheres strictly to cybersecurity laws and regulations.

5. CONCLUSION

Cybersecurity governance provides a strategic view of how an organization controls its security, including defining its risk appetite, building accountability frameworks, and establishing who is responsible for making decisions. Effective governance will ensure that cyber security activities help to support the organization's strategic goals.

REFERENCES

[1] Turner, D., Fossi, M., Johnson, E., Mack, T., Blackbird, J., Entwisle, S., ... & Wueest, C. (2008). "Symantec Global Internet Security Threat Report–Trends for July-December 07." Symantec Enterprise Security, 13, 1-36.

[2] Chinelo, N. S., & Ejike, A. A. (2022). "Security Challenges and the Implications on Business Sustainability in Nigeria." E-Journal, Spring, 1-16.

[3] An introduction to Cybersecurity: A Beginner's Guide by Simplilearn : Last updated on Apr 25, 2023 https://www.simplilearn.com/introduction-to-cyber-security-beginners-guide-pdf

[4] Governance Today | ABN: 75 159 265 175. https://governancetoday.com/

[5] Definition of Framework; dictionary 2023. https://dictionary.cambridge.org/dictionary/english/framework

[6] Posthumus, S., Von Solms, R., & King, M. (2010). "The Board and IT Governance: The What, Who and How." South African Journal of Business Management, 41(3), 23-32.

[7] Symons, C., Cecere, M., Young, G. O., & Lambert, N. (2005). "IT Governance Framework Structures: Processes and Communication."

[8] Gashgari, G., Walters, R. J., & Wills, G. B. (2017, April). "A Proposed Best-Practice Framework for Inf ISO-CASCO_0.Explanatory note and overview on ISO Survey 2021 results.pdformation Security Governance." In IoTBDS (pp. 295-301).

[9] ISO. (2021). The ISO survey of management system standard certifications. ISO-CASCO_0.Explanatory note and overview on ISO Survey 2021 results.pdf
[10] Brenner, J. (2007). "ISO 27001 Risk Management and Compliance." Risk management, 54(1), 24-29.
[11] "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework." Published on Jan 19, 2023. https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf
[12] Symons, C. (2005). IT governance framework. *FOrrester research*.
[13] COBIT, C. (2005). IT Governance Institute. *Control Objectives for Information and related Technology (COBIT 4.0)*.
[14] What is ITIL and how can best practices help you? https://www.opservices.com/o-que-e-o-itil/
[15] Security Training https://br.pinterest.com/pin/377317275031517271/