International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Security Risk Assessment in a Hybrid Data Center

Tinashe Blessing Chuwe[1], Mainford Mutandavari[2]
Department of Information Technology, Department of Software Engineering
Harare Institute of Technology University
Harare Institute of Technology, P.O Box BE277, Belvedere Harare

Abstract: **In today's world of cloud computing, in which internet-based data is managed from remote locations, all data is entered, saved, processed, and backed up on central servers. The data center is a location where all of these servers are assembled, thanks to technological breakthroughs. Though some Data Centres have been supported through several security measures: security policies and legislation, advanced technical hardware, and software security solutions, incidents of security attacks continue to mount raising questions on the adequacy of the security processes. This paper will look at: i) data center security and the frameworks that are used to manage security concerns, ii) robust information technology (IT) security risk assessment frameworks as one of the measures that may improve the security posture of hybrid data center. iii) A bibliometric analysis was used to identify the journals that published articles related to data center security and risk assessment frameworks.**

Keywords: - Data Center, Risk Assessment, Resilience, Security, Virtualization, Infrastructure

I. INTRODUCTION

With the advancement in technology, data centers face many risks on regular basis, in addition these dangers may have severe effects on the daily processes of the data center. The data center integrates the organization's shared IT infrastructure with the main objective of storing, processing, and transferring data and applications. [1] a risk assessment is required to identify and analyze the facility's current level of resilience. In addition to making sure critical business applications can keep operating, it is important to plan for future capacity that matches up with its future growth plans. A risk assessment must be done at least every two years, or if there is a change in the infrastructure, as certain firms are obliged to demonstrate regulatory compliance and meet local criteria. Data center risk assessment can also help organizations benchmark against leading practices and standards and better understand their risk landscape.

II. LITERATURE REVIEW

The researcher examines the literature on security risk assessment in Data Centers that have been generated by other authors and academics and clearly reveals the researchers contributions to the field of cybersecurity.The researcher's work is found in other researchers.[2]a literature review is a method in which a researcher gathers and reviews existing studies to gain a detailed understanding of the subject matter.

A. Security Risk Assessment Process

The security risk assessment approach is used to determine an organization's strengths and weaknesses on the systems, as well as to identify and reduce threats to a level that is acceptable in terms of the organization's security standards[3]. For example, ensuring a certain level of confidence in the confidentiality, integrity, and availability of their application and the data it processes could be one of an organization's security needs[3]. Risk assessment focuses on determining the possibility of a negative event (for example, a data breach or unauthorized access) and the impact it will have on the system's and organization's exploitation. Risk mitigation methods are devised and established after this evaluation to reduce the possibility and impact of the risks. Prior to carrying out any risk assessment process, data center managers may follow a risk assessment framework, which serve as a roadmap for the risk assessment process to be carried out by the organization[3].

B. Operationally Critical Threat, Asset And Vulnerability Evaluation (OCTAVE) Framework

In [4] the Software Engineering Institute (SEI) developed the OCTAVE strategy to solve the information security risks that various organisations might face.[4] OCTAVE is an approach for identifying, managing, and evaluating information security threats. The OCTAVE methodology is aimed especially at those who are in charge of controlling an organization's operational risks, data center managers included. SEI created the initial OCTAVE Framework method in 1999 in response to growing concerns about risk management, particularly risk assessment.[5] This architecture was designed for large companies with more than 300 people that have a multi-layered hierarchy and manage their own software infrastructure[5]. OCTAVE is a flexible and self-directed risk assessment methodology and the framework defines assets as including people, hardware, software, information and systems. All these elements are found in the data center [5]. The framework was intended to help businesses make the best decisions they can depending on the risks they face.

OCTAVE looks at both organizational and technological concerns to provide a full view of an organisation's threat landscape. The evaluation criteria for this framework are centered on a three-phased technique[4] , each is intended to deliver tangible outcomes for Data center managers. The stages are as follows:

Stage 1 : [4] Security Requirements for the Entire Organization.

Stage 2: Identify[4] Infrastructure Vulnerabilities[4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Stage 3: Determine a Security Risk [4]Management Strategy.

During Stage 1, assets of information and their values, threats to those assets and security requirements are recognized based on the knowledge of personnel from a variety of sources from multiple levels within the Data center, along with standard catalogues of data.[4] For instance, known threat profiles and good organization's assets, threats and current protection strategies. [4] This information may then be used to define an organization's security requirements, which is what OCTAVE's first phase is all about.

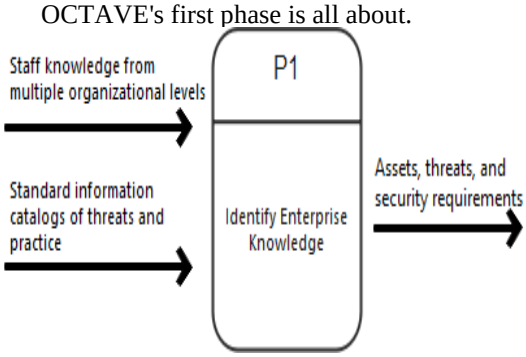

Fig. 1 OCTAVE Stage 1

Stage 2 of OCTAVE [4] builds on the data collected in Stage 1 by mapping the organization's information assets to information infrastructure components (both the physical and networked IT environments) in order to identify high-priority infrastructure components. The infrastructure is then subjected to a vulnerability assessment in order to identify weaknesses. The infrastructure vulnerability evaluation is based on common catalogs of information, such as standard intrusion scenarios and vulnerability information, same as it was in Stage 1. Phase 2 concludes by determine which infrastructure components are of the utmost importance, lacking policies and practices, and vulnerabilities.[4]

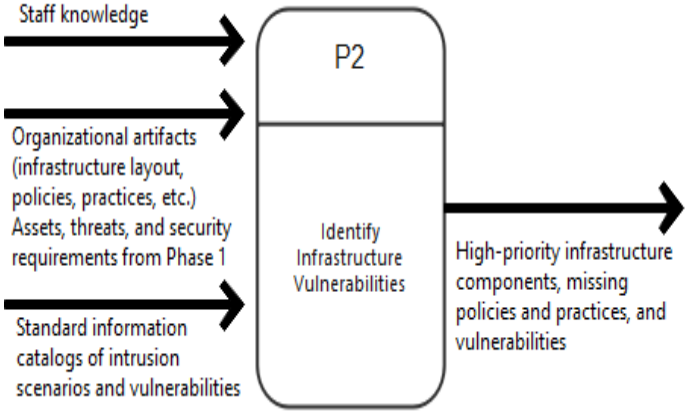

Fig. 2 OCTAVE Stage 2[4].

[4] OCTAVE's Stage 3 builds on the data collected in Stages 1 and 2. The assets, threats, and vulnerabilities identified in OCTAVE's earlier phases are analysed in the context of conventional intrusion scenarios to identify risks. The risk's impact and likelihood (also known as risk attributes) are calculated and then utilized to assist prioritize the risks. Phase 3's goals include developing a protection strategy for the enterprise and establishing a complete plan for managing security risks based on the prioritized list of threats and information from previous stages[4].

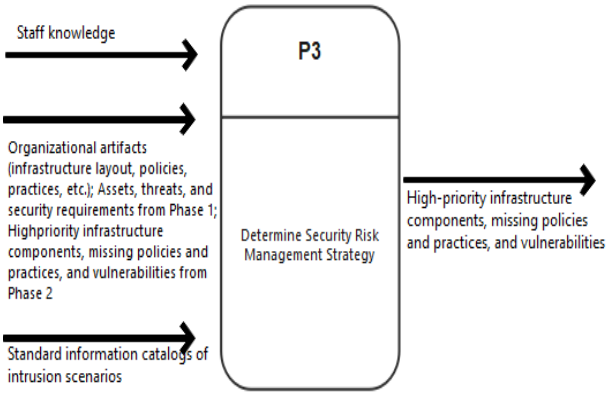

Fig. 3 OCTAVE Stage 3.

The primary goal of OCTAVE is to help businesses connect their goals and objectives with their information security activities. The main benefit of using OCTAVE framework in risk assessment is that it provides a formal and systematic process for analysing the risks that data center administrators encounter, making it easier for them to adapt[5]. A formal risk assessment process enables administrators within the data center to implement controls only where they are needed[5].

Data centers contain a big amount of valuable data and cutting-edge equipment, hence they are usually vulnerable targets..[1] investigated information security risks across countries in the Gulf with a focus on Saudi Arabia and noted that most of the countries have allocated huge budgets for information security and in development and deployment of high-performance computing environments without the use of correct cyber security risk managing frameworks. The study found that failure to adopt a clear information security threat management, the existing massive investments in addressing information security risks may be rendered ineffective by this paradigm. The author bemoans the fact that the situation has gotten worse due to a lack of research on how security risks for high-performance computing centers might be improved and managed.[1] and [6] underscore that existing risk management frameworks are generic and less applicable for different countries. [1] Some security risk management frameworks are Euro-centric and do not take into account the needs of other countries. The uptake and success of the use of frameworks for risk management developed outside these regions have been slow because of cultural and contextual differences in these regions.

[7] sought to demonstrate the resource availability challenges emanating from security risks of virtualized environments through exploring hybrid data centers across the globe. The study came to conclude that virtualized data centers have deteriorated performance in delayed sensitive applications. The delays arise from queuing mechanisms and variations from cyber security attacks. [7]then proposed a cybersecurity risk assessment framework for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

such environments which may enable reduce and even mitigate the risks arising in such settings.

Recent studies outlined by [8] provides a complete structure for the analysis and treatment of risks in supercomputing systems in response to the multiplicity of escalating security issues. The author propounds that security risk assessment is a prerequisite for modern advanced supercomputing environments that are characterized by combining traditional and virtualized infrastructure — such modern infrastructure is becoming one of the most sought-after targets for hackers and cybercriminals[8].

[9] then articulates a step-by-step methodology of implementing the security assessment framework by way of first identifying the purpose of the framework, identifying the target audience, defining the risk assessment methodology (asset identification, identification of threats and weaknesses, analysis of the controls, assessment, and acceptance criteria, and procedures of handling the risks. According to the previous authors, without a suitable security risk assessment framework, today's supercomputing infrastructure is at risk of being exploited by threat performers. It implies that most of these supercomputing centers might fail to attain their purported benefits and objectives.

The hybrid structure has introduced a novel set of security concerns that must be addressed.[10] argues that computer security for the supercomputing environment is not just a matter of implementing security policies, developing a raft of regulatory and legal frameworks or implementing waterproof technical security hardware and software, but an organized approach that takes into consideration the entire spectrum of security risks in a hybrid data centers. The author argues that the continued investment in supercomputing systems without clearly identifying measures to protect the same might not result in the anticipated benefits.

Adopting current technologies as a means of lowering costs and increasing efficiency is a good idea. However, these new technologies introduce certain new security vulnerabilities. [11]suggest that in terms of infrastructure security, building a framework, risk-driven enterprise security, and information assurance architectures are critical. In conclusion, the author's proposed the application of multi-layer security architecture.

A secure and healthy facility will act as a foundation for a successful enterprise in the 21st century. [11]]argues that HPC facilities have treated security as an afterthought in a world where performance is the number one priority. The paper presents a security architecture and associated security best practices for the Datacenter. The architecture aims to mitigate the risks about High Performance Center (HPC) facility[11]. According to the author, proper security options must be included in the security of computer networks and their overall functionality.[12] States that organizations should understand that the most dangerous threats may come from where they least expect them. The report suggests that securing data centers must focus on a combination of physical measures and logical security to thwart cyber intrusions. As a result, both security approaches might be utilized in data centers to increase resilience.

Data centers are the core of cloud computing and services. Both conventional and completely virtualized infrastructure have been blended into hybrid data center architectures. [13] the study addresses the emerging risks by conducting a complete risk assessment using the National Institute of Standards and Technology (NIST) framework. The study explores resource availability problems originating from delay variants and queuing mechanisms found in virtualized systems and their bearing on the delay-sensitive application. According to the findings, virtualized data centers have degraded performance in time-sensitive applications. The researcher concludes that, the benefits of computing infrastructure can hardly be isolated from its associated security needs.

Identifying threats and managing risks associated with data centers has become a key responsibility for businesses. To avoid potential risks and damages, companies will need to focus their resources on damaging threats.[14] This paper discussed an exploratory study of the major ICT security threats to data centers of 33 government organizations. They are 8 categories of common threats that occur in Malaysian Public Sector facilities.

These threats were used in this study to identify their frequencies and to determine their ranking and to identify their causes. It was discovered that technical threats, stand as the major threats encountered by organizations on regular basis. The main sources of these threats were identified as lack of resources in terms of budget and skilled personnel, lack of manpower on security issues, lack of user awareness and education, weak policies, and deliberate attacks by hackers.[14] In conclusion, this study has successfully identified major ICT security threats only that are regularly faced by data centers in the Malaysian public sector.

[15]argues that data center hazards have changed over the past few years from construction issues to operational issues. As a result, data center operators must have a full understanding of all hazards and their facets. In [15]he goes on to say that a data center is an ecosystem in which players can put other consumers at danger. The author [15] concluded that, security measures need to be worked on at all levels, not just on the physical one. Also Data center operators need to integrate their customers and suppliers into their daily processes in order to understand the risks so as to protect everyone [15].

III. CONCLUSION/FUTURE WORK

Security is a process, not a product. Therefore data center managers should strive for a resilient data center to known attacks at any given time since new attacks are emerging every day. Many security vulnerabilities exist in data center facilities, which may necessitate a re-evaluation of well-known threats based on existing architectures. Literature survey indicates the need for implementing robust information technology (IT) security risk assessment frameworks as one measure that may improve the security posture of such information technology equipment. However, these prescriptive solutions are generic and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

largely Western-oriented rendering them less applicable in the Zimbabwean context. In future study testing of the proposed frameworks with real threats specific to a given data center is of paramount importance and needs to be considered.

ACKNOWLEDGMENT

This review paper and the research behind it would not have been possible without the exceptional support and guidance of my supervisor, Mr. Mutandavari. Special thanks to all stakeholders who assisted me on this review paper.

REFERENCES

[1] M.A, "Supercomputers can spot cyber threats," 2019.

[2] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," *J. Plan. Educ. Res.*, vol. 39, no. 1, pp. 93–112, 2019, doi: 10.1177/0739456X17723971.

[3] A. Sen, "Scholars ' Mine Security risk assessment in cloud computing domains," 2018.

[4] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0," 1999.

[5] P. Eric LACHAPELLE and P. Fitim RAMA, "Risk Assessment with OCTAVE," 2015. https://pecb.com/whitepaper/risk-assessment-with-octave.

[6] S.Peisert, "Cyber security for HPC Systems: State of the art and looking to the future," 2018.

[7] G. S. and A. S. D. Bufnea, V. Niculescu, "Babes-Boyai University's High Performance Computing Center, Informatica.," vol. 61, no. 02, 2016.

[8] N. Alshareef, "A model for an information security risk management (ISRM) framework for Saudi Arabian organisations," *Int. Conf. ITS, ICEduTech STE 2016*, pp. 365–370, 2016.

[9] M. V. M. S.Janosepah1, N.Modiri2, "Data Center Tiers Security Service," 2014.

[10] C. Cimpanu, "Supercomputers hacked across Europe to mine cryptocurrency," 2020.

[11] P. Mcmahon and A. Hutchison, "A security architecture for high performance computing facilities," *Proc. Inf. Secur. South Africa, Balalaika Hotel. Sandton, South Africa.*, 2006.

[12] K. POLIT, "Data Center Security Must Focus on Physical and Logical Security," *info@meritalk.com*, 2021. .

[13] F. Munodawafa and A. I. Awad, "Security risk assessment within hybrid data centers: A case study of delay sensitive applications," *J. Inf. Secur. Appl.*, vol. 43, pp. 61–72, 2018, doi: 10.1016/j.jisa.2018.10.008.

[14] I. Shammugam, G. N. Samy, P. Magalingam, N. Maarop, S. Perumal, and B. Shanmugam, "Information security threats encountered by Malaysian public sector data centers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1820–1829, 2021, doi: 10.11591/ijeecs.v21.i3.pp1820-1829.

[15] G. Simon, "UNDERSTANDING AND MITIGATING RISKS TO DATA CENTER OPERATION." https://www.dotmagazine.online/economic-engine-digital-infrastructure/mitigating-risks-to-data-center-operation (accessed Nov. 11, 2021).