World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review

Felix C Aguboshim [1,*], Ifeyinwa N Obiokafor [2] and Anastasia O Emenike [3]

[1] *Federal Polytechnic, Oko Nigeria.*
[2] *Anambra State Polytechnic, Mgbakwu. Nigeria.*
[3] *General studies department, The Polytechnic, Ibadan. Oyo state, Nigeria.*

World Journal of Advanced Research and Reviews, 2023, 17(02), 378–385

Publication history: Received on 17 November 2022; revised on 05 February 2023; accepted on 07 February 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.2.0154

Abstract

Data are now valued as the new oil that powers the world economy. Globally, Big data technologies have intensified the need for Sustainable Data Governance (SDG). Significant empirical evidence from literature revealed that about 2.7 zettabytes of data now in the digital universe are being threatened by cybercrime incidents that are on the rise globally. Despite the importance of SDG and cyber security, only 67% of organizations globally deployed data governance or data intelligence solutions, while 46% including Nigeria had no formal governance strategy in place. This study highlights strategies to leverage good security measures for SDG. The authors adopted the Data Management Association (DAMA) International Guide to the Data Management Body of Knowledge (DMBOK) (DAMA-DMBOK) as a conceptual framework for this study. The narrative review methodology was adopted, where related research findings from peer-reviewed articles are used to draw holistic findings that revealed significant information on strategies for leveraging excellent security practices within SDG for economic empowerment. Results show that data governance, a fundamental part of cyber security, ensures that the right people have the right access, while Information Security ensures that Enterprise Data is safe and locked down. Cyber security is at the core of ensuring confidentiality, integrity, and availability of organizations' data and leveraging data governance program that ensures that safe data is accessible across the organization in a controlled manner. The result of this study may increase understanding, and awareness of the need for information security to leverage SDG required for economic empowerment.

Keywords: SDG; DAMA-DMBOK; Cyber-security; Cybercrime; Big data

1. Introduction

Information security remains a critical activity within today's organizations in the light of continued data breaches, systems outages, and malicious software [13]. In order to truly address the subject of organization data quality: data confidentiality, integrity, and availability, in a sustainable manner, an enterprise data governance strategy needs to be adopted coupled with enterprise information security. This study examines, within the field of information systems security, the use of organizational data decision rights, rules, protocols, and policies that specify how users of information and technology resources should behave in order to prevent, detect, and respond to security incidents that may challenge SDG. SDG for effective information systems security management of organizational data depends on improving protective technology and policy compliance among data networks and employees [19], [27], and [47]. Existing information systems security management models have overly emphasized the rationality of decision-makers [19], and decision rights, rules, and protocols for data and data-related processes [16].

*Corresponding author: Felix C Aguboshim

The rise of big data has led to many new opportunities for organizations to create value from data [5] and [9]. This increasing dependence and value on data also pose many challenges for organizations. Such challenges include, among others, connecting and integrating data from numerous sources [48], data complexity [52], data security [54], data capture [12], data scale, data mobility, data value, and data analytics [29]. These challenges are handled by establishing data analytics governance, implemented through regular audits of the current data management process, adequate training for organization personnel, and implementation of sound data management and data security strategies [27] and [47]. Data Governance (DG) is comprised of systems that define decision rights, rules, and protocols for data and data-related processes, that focus on the people, technology, and processes that are involved in the creation, management, and stewardship of enterprise data performed according to agreed-upon models that define the protocol for actions with what, when, and under what circumstances to use what methods for ensuring the effective and efficient use of quality data [16] and [23]. Data Governance and enterprise information security are so tightly entwined. The process of maintaining sustainable data governance, new technologies, security trends, and threat intelligence could be a challenging task.

Globally, especially in the last decades, digital records protections have become ubiquitous [47]. A good concept for information security addresses three major objectives namely confidentiality, integrity, and availability of enterprise data. Safeguarding information and other assets from cyber threats, which take many forms such as malware (a style of malicious software within which any file or program will be accustomed to harm a mortal), worms, viruses, Trojans, spyware, ransomware, social engineering (an attack that relies on human interaction to trick users into breaking security procedures to realize sensitive information that's typically protected), phishing (a variety of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent). Others include spear phishing, insider threats, distributed denial-of-service (DDoS) (attacks where multiple systems disrupt the traffic of data flow in a targeted system, like a server, website, or other network resources, by submerging the target with dispatches, connection requests, or packets, with the intention to decelerate the system, crash it, or preclude a licit business from using organization data. Other common attacks include Advanced patient pitfalls (APTs), Man-in-the-middle (MitM), botnets, drive-by-download attacks, exploit accouterments, malvertising, vishing, credential filling attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC), email spoofing, brute-force attack, dictionary attack, salami attack, and zero-day exploits.

Modern enterprise information security systems are now available such as firewalls, intrusion detection and prevention, anti-malware, and a plethora of other systems that are now standard elements of today's networks that can if properly implemented, in a properly joined-up manner with good data governance can prevent attackers from slipping between the cracks. It is not enough to be conscious of these concepts of multi-layered security solutions and how our networks can be protected, it is important to know what is on our network, the adequacy of our security measures, and how appropriately our security measures are leveraging data confidentiality, integrity, and availability. Without an understanding of our network, data governance strategies, and the state of security on our devices, we may not be able to mitigate global data security challenges that may threaten sustainable data governance. Identifying the cause of data breach is as important as identifying with certainty where the breach, stolen, or leaked data came from. This is because if cybercrime security personnel cannot identify with certainty where the breach, stolen, or leaked data came from, it will be much more difficult, if not impossible, for them to identify the cause of the data breach. Investigating data breaches also involves the collection of data widely encompassing that spans organization data, including shared files among staff members, company-owned or bring your own device (BYOD), and other unmanaged locations. This takes time even in SDG systems. Data can also be collected from randomly selected samples of devices, which risks missing the compromised systems. This study highlights strategies to leverage good enterprise security measures for SDG.

1.1. Problem Statement

Data Governance and enterprise information security are tightly interwoven. DG, a proactive means to minimize risk [50], is the process of managing the availability, usability, integrity, and security of the data in enterprise systems, based on internal data standards and policies that also control data usage [45]. Effective data governance, a fundamental part of cyber security, ensures that enterprise data are consistent and trustworthy, accessed by the right people, and not misused; while information security ensures that enterprise data is safe and locked down. The general IT problem postulated in this study was poor data governance, which is a fundamental part of cyber security performance or sustainability of DG majorly due to poor data intelligence solutions and security measures for SDG in Nigeria. The specific IT problem is that some cyber security and enterprise information security managers in Nigeria lack strategies to enforce good security measures, standards, laws, guidelines, and value systems for SDG.

1.2. Research Question

What are the appropriate enterprise information security systems to mitigate global data security challenges in our networks, and data governance strategies, in order to leverage sustainable data governance in Nigeria?

2. Literature Review

Data Governance, which is now a global discourse, is about realizing that data are the means to any organization's wellbeing [11] and [18], innovated on three critical generalities: the people, technology, and processes [19], [27], and [47], involved in the creation, operation, and stewardship of enterprise resources that enabled the applicable running of the data across the organization. It further refers to the foundation of the people, technology, and processes that hold decision rights that are held responsible for an organization's decision-making about its data, users of the data, and circumstances, and protocols to be followed in using the data. Data governance is seen as the framework for assigning decision-related rights and duties in order to adequately handle data as an organizational asset [27], and provide for data integrity, data security, vacuity, and thickness, while guarding high-quality data throughout the lifecycle of that data [11]. The main driver for data governance is considering data as an asset or productivity of the organization [27] and [47].

The data governance framework includes knowledge creation and strategies for data operation, preservation, curation, availability, quality issues, as well as legal and policy enterprises over data governance and data security [23]. Data governance is a decision-making process concentrated on authority structure to specify decision rights and responsibilities that encourage queries or actions regarding data use, security, integrity, and vacuity. The emergence of big data technologies to design public policy and deliver public services has necessitated the need for organizations to design data policy and governance [8] and [22]. Data governance conditions arise from consequential problems related to using digital technologies grounded on massive volumes of data, shaping tools to reduce participating pitfalls, and defining patterns for stewards' and analysts' actions [31] and [37]. Working with big data requires data governance to promote ease of use, security, norms, guidelines, and rules. Information systems security failures have dire consequences on SDG, including commercial liability, loss of credibility, and financial damages.

Security-related information integration has also become feasible in this increasingly digital and interconnected world. Computers and information systems are crucial to SDG in any organization. Ensuring the security of these systems is a vital task that maintains the basic aspects of the information security phenomenon, namely, confidentiality, availability, and integrity [25]. Data governance and enterprise information security are so tightly entwined [46], in the sense that data governance when aligned with new data security governance practices will help to solve data governance problems. Also, aligning data governance practices and proposals to key strategic initiatives like information security will further enhance SDG. Successful data governance in any organizational process is heavily dependent on the effective implementation of IT resources that ensure wide-ranging means of security control platforms. Security controls include asset management measures, vulnerability management measures, and incident management measures [51].

Significant empirical evidence from literature revealed that the ubiquitous alarming rate of digital data flow requires the deployment of data governance or data intelligence solutions, a situation theorized by [32], as the "datafication" of society, where digital data can easily be produced, stored and processed in a way that has no historical precedent. Significant empirical evidence from literature revealed that with the volume of data flow and the latest advances in technology, such as the Internet of Things (IoT), the digital universe is being threatened by cybercrime incidents that are on the rise globally [30], [32], and [43]. It is required that organizations take a holistic view as to how they secure information and services, since these technologies may have the least complexity and are unlikely to be innately secure [30] and [53]. DG is an emerging subject in information system security in recent years, following the dramatically increasing volume of data used within organizations and the critical role data play in business operations. Organization enterprises have become exposed and increasingly susceptible to information leakages, data thefts, cyber-attacks, and sabotage [43]. This also results in a rapidly increased volume of e-waste that might contain confidential information of a different nature, which results in ecological security or electronic waste security [3] and [4].

Data governance, coupled with information system security can be deployed to detect cyber security incidents such as Intrusion Detection, Man-in-the-middle, and DDoS attacks, and make guarantee the security of sensitive data in enterprise information systems [43] and [53]. While Data governance represents the framework and core capability for data management [7] and [15], which assures that all operational functions of data management contribute to achieving organizational objectives, and strategy [12]. Data management depicts a practical implementation of data-related activities on the operational level [21]. All data management activities by stakeholders are designed to ensure data consistency and integrity, function goals, and responsibilities for effective and efficient organization values [2]. Data management activities also ensure confidentiality, integrity, and availability of the right data at the right time for an

effective decision-making process [1] and [40]. This requires the transformation of the enterprise culture to a risk-based culture, where digital security is the responsibility of all the employees of the enterprise [41].

2.1. Conceptual Framework

We adopted the Data Management Association (DAMA) International Guide to the Data Management Body of Knowledge (DMBOK) (DAMA-DMBOK) as a conceptual framework for this study. DAMA-DMBOK was proposed by [14]. DAMA-DMBOK defines a standard organizational view of data management functions, terminology and best practices, planning, oversight, and control over the management of data and the use of data and data-related sources [14]. DAMA provides the foundation for data management known as DAMA-DMBOK [15], and describes data management functions that cover all the aspects of data architecture, development, management, and governance. DMBOK is a comprehensive guide to international data management standards and practices for data governance and management professionals. Data governance is a set of processes, responsibilities, and tools that provides practices for an enterprise-wide perspective on managing data as an organizational asset [27] and [47]. These practices enable the effective delivery of high-quality data that improve regulatory reporting and ensures compliance with regulatory requirements. High-quality data enhance operational efficiency which, subsequently, results in cost reduction and value creation for the organization. DAMA-DMBOK is a set of best practices of data management recommended for implementation in an organization [35]. The DAMA-DMBOK provides guidance for activities, which should be performed or taken into consideration for each data management and data governance area. Data Governance is limited to the three data management areas according to the [15], which are data governance, data quality, and metadata, but stands at the center of the data management model to govern and coordinate the operational aspects of data management [39]. The main objective of data governance is to get value from data – to monetize data and meet compliance and regulatory reporting requirements [49]. DAMA-DMBOK was adopted as our conceptual framework and theoretical foundation to study security issues associated with data governance in the era of global data security challenges, especially in Nigeria.

3. Research Methodology

This study incorporated the use of a narrative review approach that aligns with the consensus of many researchers on the narrative review research methodology approach. The consensus of many researchers on narrative review research methodology is that it is best suitable for comprehensive studies which aim at synthesizing a stream of research, identifying problems, gaps, and research opportunities within it, and providing a foundation for drawing holistic interpretations or conclusions, and significant interpretations based on the existing theories, conceptual framework, and models within the review boundaries [24], [34], and [36]. Data do not speak for themselves, and so must be narrated [20]. The narrative review approach involved the review, analysis, and integration of different, related, and interactional approaches and research findings [17] and [44], with the aim of exercising a holistic-content reading and drawing holistic interpretations or conclusions [10] and [36], based on the reviewers' own experience, existing theories, and models that may answer the research question. A narrative study approach is most appropriate for a descriptive or explanatory study that allows for a narrative-constructivist and integration approach [17], uses mainly narrative methods of data collection and analysis, and produces a final narrative report [20]. Narrative review methodology provides significant strengths that have the ability to establish platforms for the comprehension of diverse and numerous understanding derived from multiple data sources and research findings. It also avails the researcher, the opportunity to make reflective practices and acknowledgment of researchers' views and knowledge [42]. Methodological triangulation, a platform for engaging multiple sources of data to gain multiple perspectives, and maximize the reliability and validity of data, in order to build a coherent justification of data interpretation was also adopted. Methodological triangulation helps to confirm the reliability and validity of information collected, and justification of interpretations from the reviews.

Globally, all security platforms are complex, dynamic, and psychological. In reality, there are no perimeter boundaries, because perimeter defences, control over devices, employee adherence to policies, control over policy enforcement, and enterprise definitions are no longer reliable. Defences need to be personalized as attackers personalize their attacks. Nevertheless, organizations must recognize their enterprise systems as comprising some sort of perimeter; otherwise, the organization's security management domain becomes the entire internet. Information system security and data governance literature are vast in nature [38]. Narrative high-quality literature reviews in information system security and data governance should contain a clear articulation of the review boundaries, the steps taken to collect the relevant literature, and how the literature was synthesized and analyzed to draw holistic interpretations or conclusions [38]. Five factors impact future security perimeter measures: Cloud, Software as a service (SaaS), Software-defined networking, Big Data, and the Internet of Things (IoT) [26]. In this study, we restrict our narrative reviews to areas that

cover data governance as a fundamental part of cyber security that ensures that the right people have the right access to organization data, and, information Security that ensures that enterprise data are safe and locked down. Our review boundary for cyber security includes at the core, ensuring confidentiality, integrity, and availability of organizations' data that leverage data governance program for assurance of accessible safe data across the organization in a controlled manner, while the scope of the Data Governance Model is limitedto data quality, and metadata management.

3.1. Data Collection

Some peer-reviewed research findings from journals and other articles that are relevant to our study objectives and consistent with our research question and conceptual framework were reviewed. Our key search words were tailored toward identifying appropriate enterprise information security systems to mitigate global data security challenges in our networks thereby leveraging sustainable data governance. Our reviews incorporated 55 references. Fifty-three (96%) of the overall references incorporated within the study are peer-reviewed, while (100%) are peer-reviewed journals that are within the last 5 years. The summary is given in Table 1.

Table 1 Summary of Research Articles Reviewed

Incorporated articles	Number
Total references within the study review:	55
Total peer-reviewed references in the study:	53
Total peer-reviewed in the study within the last 5 years:	53
% Peer-reviewed references in the study:	96%
% Peer-reviewed references in the study within the last 5 years:	100%

4. Analysis, Synthesis and Discussions

Data governance requires both business and IT support because data is created and updated by business processes while using IT infrastructure [5] and [27]. To achieve value from data and maintain data-related activities in a controlled manner according to business needs and regulatory requirements, an enterprise-wide data strategy should be created. The data strategy should be aligned with business and IT strategy to support key organizational priorities, needs, and goals [5]. Each goal defined in the data strategy should be mapped to corporate strategy and should follow the corporate vision and mission. Following steps should be taken to create the enterprise-wide data strategy: (1) gathering business requirements for data, (2) mapping business requirements to both enterprise goals/strategically dimensions and IT goals, (3) mapping business requirements to the Data Governance Model areas, (4) determination of expected benefits, efficiency improvement, impacted information systems, possible solution design, (5) building of data strategy and roadmap, and (6) data strategy approval by the Data governance operational steering committee.

5. Conclusion

Information security experts should strive to be good organizational security personnel for their data. They must know where all the organization data are at any point in time, segregate them into separate sections, and ensure that the security measures between sections are sound, healthy, and secure. This segregation is desired to ensure that all sections of the organization's data are at risk. If there is any breach, in one section, the risk can be contained and most of the organization's data will be safe. Also, deleting any low-value data, according to predefined and legally, reduces risks and minimizes the volume of data that could be compromised. There should be strict compliance rules concerning how long the organization should retain its data. Data are deleted once the retention period is over, to avoid the risks and costs outweighing any residual value. Other methods to avoid organization data from being compromised included, among others: herding valuable organizational data such as organizations' intellectual property and company records and contracts stored inappropriately in file shares or email attachments. Company data records managers and end-users should ensure that records are always filed correctly via appropriate data governance schemes. Organizations can adopt information governance technology that leverages excellent enforcement of data security by increasingly enforcing strict regulations surrounding data privacy and financial information. Important personal, financial, and health details are to be stored in controlled repositories. All critical value data should be stored securely and only in secured locations. Even when such data are disposed of correctly, they may still be retained in back-ups or archives. To enforce data security, there should be regular sweeps of email, file shares, and other unprotected systems to enable organizations to quickly locate and remediate unprotected private data. Finally, good access control should be

maintained, coupled with sound policy and constant vigilance to ensure that only people who can access high-risk or high-value data are those who require it for day-to-day work. The use of Blockchain can enhance security, privacy, and optimization of the entire services because blockchain offers secure application development with smart contracts and its distributed technology [6], [28], and [55] especially for a new development of pioneering research [33] and [55].

Compliance with ethical standards

Acknowledgments

Our sincere appreciation and thanks to Dr. Felix. Chukwuma.Aguboshim for his wonderful contributions.

Disclosure of conflict of interest

The authors had no potential conflict of interest.

References

[1] Abraham, R., Schneider, J., & VomBrocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49(1) , 424–438. https://doi.org/10.1016/j.ijin fomgt.2019.07.008

[2] Alansari, Z., Anuar, N. B., Kamsin, A., Soomro, S., Belgaum, M. R., Miraz, M. H., Alhassan, I., Sammon, D., & Daly, M. (2018). Data governance activities: A comparison between scientific and practice-oriented literature. Journal of Enterprise Information Management, 31(2), 300–316. https://doi. org/10.1108/JEIM-01-2017-0007

[3] Alghazo, J., Ouda, O. K. M., & El Hassan, A. (2018). E-waste environmental and information security threat: GCC countries vulnerabilities. Euro-Mediterranean *Journal for Environmental Integration, 3*(13), 1–10. https://doi.org/10. 1007/s41207-018-0050-4

[4] Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021).Information security as a national security component.*Information Security Journal: A Global Perspective, 30*(1), 1-18. https://doi.org/10.1080/19393555.2020.1795323

[5] Alhassan, I., Sammon, D., & Daly, M. (2019).Critical success factors for data governance: a telecommunications case study. *Journal of Decision Systems, 28*(1), 41-61. https://doi.org/10.1080/12460125.2019.1633226

[6] Alketbi, A., Nasir, Q., & Talib, M. (2018).Blockchain for government services—Use cases, security benefits and challenges. *In IEEE 2018 15th Learning and Technology Conference (L&T)*, 112–119

[7] Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018).A systematic literature review of data governance and cloud data governance. Personal and Ubiquitous Computing 23(5–6) , 1–21. https://doi.org/10.1007/s00779- 017-1104-3

[8] Ataç, C., & Akleylek, S. (2019). A survey on security threats and solutions in the age of IoT.*European Journal of Science and Theology, 15*(1), 36–42. https://doi.org/10.31590/ejosat. 494066

[9] Baijens, J., Huygh, T., & Helms, R. (2021). Establishing and theorising data analytics governance: a descriptive framework and a VSM-based view.*Journal of Business Analytics*, https://doi.org/10.1080/2573234X.2021.1955021

[10] Baker, J. D. (2016). The purpose, process and methods of writing a literature review: Editorial. *Association of Operating Room Nurses. AORN Journal, 103*(3), 265-269. https://doi.org/10.1016/j.aorn.2016.01.016

[11] Brockman, C. (2020). Data security governance explained. https://cybersecurity.att.com/blogs/security-essentials/data-governance.at-the-heart-of-security-privacy-and risk#:~:text=Data%20governance%20is%20the%20capability, security%2C% 20availability%2C%20and%20consistency.

[12] Brous, O. P., & Janssen, M. (2020). Trusted Decision-Making: Data Governance for Creating Trust in Data Science Decision. Administrative Sciences, 10(1), 81-100. https://doi.org/10.3390/admsci10040081

[13] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

[14] DAMA. (2009). DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide).https://damadach.org/dama-dmbok-functional-framework/

[15] DAMA. (2017). DAMA-DMBOK Data Management Body of Knowledge, Technics Publications.

[16] Data Governance Institute. (2015). Definitions of Data Governance. Retrieved April 9, 2022 from : http://www.datagovernance.com/adg_data_governance_definition/.

[17] De Fina, A. (2021). Doing narrative analysis from a narratives-as-practices perspective.*Narrative Inquiry, 31*(1), 49-71. https://doi.org/10.1075/ni.20067.def

[18] DeStefano, R. J., Tao, L., & Gai, K. (2016). Improving Data Governance in Large Organizations through Ontology and Linked Data. Proceedings IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). https://doi.org/10.1109/cscloud.2016.47

[19] Dong, K., Lin, R., Yin, X., & Xie, Z. (2021). How does overconfidence affect information security investment and information security performance? *Enterprise Information Systems, 15*(4), 474-491. https://doi.org/10.1080/17517575.2019.1644672

[20] Dourish, P., & Gómez Cruz, E. (2018). Datafication and data fiction: Narrating data and narrating with data. *Big Data & Society*. 1-10. https://doi.org/10.1177/2053951718784083

[21] Engels, B. (2019). Data governance as the enabler of the data economy.Intereconomics, 54(4), 216–222. https://doi.org/ 10.1007/s10272-019-0827-y

[22] Filgueiras, F., & Lui, L. (2022). Designing data governance in Brazil: an institutional analysis.*Policy Design and Practice,*1-16. https://doi.org/10.1080/25741292.2022.2065065

[23] Gupta, N., Blair, S., & Nicholas, R. (2020). What We See, What We Don't See: Data Governance, Archaeological Spatial Databases and the Rights of Indigenous Peoples in an Age of Big Data, Journal of Field Archaeology, 45:sup1, S39-S50, DOI: 10.1080/00934690.2020.1713969

[24] Hill, C., & Burrows, G. (2017). New voices: The usefulness of a narrative approach to social work research. Qualitative Social Work: Research and Practice, 16(2), 273-288. https://doi.org/10.1177/1473325017689966

[25] Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems, 60*(3), 201-211. https://doi.org/10.1080/08874417.2018.1432996

[26] ISACA. (2018). ISACA Perspective: Five Factors Affecting Today's Security Perimeter Defenses. Retrieved from https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2018/isaca-perspective-five-factors-affecting-todays-security-perimeter-defenses

[27] Karkošková, S. (2022). Data Governance Model To Enhance Data Quality In Financial Institutions, *Information Systems Management*, https://doi.org/10.1080/10580530.2022.2042628

[28] Kaur, H., Alam, M., Jameel, R., Mourya, A., & Chang, V. (2018).A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment". *Journal of Medical Systems, 42*(8), 156. https://doi.org/10.1007/s10916-018-1007-5

[29] Lis, D., & Otto, B. (2020). Data Governance in Data Ecosystems – Insights from Organizations*..AMCIS 2020 Proceedings.12*(1). https://aisel.aisnet.org/amcis2020/strategic_uses_it/strategic_uses_it/12

[30] Loft, P., He, Y., Janicke, H., & Wagner, I. (2021). Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis, *Enterprise Information Systems, 15*(4), 448-473. https://doi.org/10.1080/17517575.2019.1605000

[31] Madison, M. (2020). "Tools for Data Governance." Technology and Regulation 2020: 29–43. doi: 10.26116/techreg.2020.004.

[32] Maffei, S., Leoni, F., & Villari, B. (2020). Data-driven anticipatory governance. Emerging scenarios in dataforpolicy practices. *Policy Design and Practice, 3*(2), 123-134. https://doi.org/10.1080/25741292.2020.1763896

[33] Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Ogu, I., Aliper, A., Romantsov, K., Zhebrak, A., Ogu, I. O., & Zhavoronkov, A. (2018). Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget, 9*(5), 5665. https://doi.org/10.18632/oncotarget.22345

[34] McCabe, A., & Van De Mieroop, D. (2021). Methodology of narrative study.*Narrative Inquiry, 31*(1), 1-3. https://doi.org/10.1075/ni.20137.mcc

[35] Murti, Z., Andarrachmi, A., Hidayanto, A. N., & Yudhoatmojo, S. B. (2018). Master data management planning: (Case study of personnel information system at xyz institute). Proceedings of 2018 *International Conference on Information Management and Technology, ICIMTech 2018 Jakarta, Indonesia (IEEE)*, 160–165. https://doi.org/10.1109/ICIMTech.2018.8528185

[36] Nasheeda, A., Abdullah, H. B., Krauss, S. E., & Ahmed, N. B. (2019). Transforming Transcripts Into Stories: A Multimethod Approach to Narrative Analysis. *International Journal of Qualitative Methods,* https://doi.org/10.1177/1609406919856797

[37] Özdemir, V., & Hekim, N. (2018). Birth of industry 5.0: Making sense of big data with artificial intelligence, "the internet of things" and next-generation technology policy. OMICS: *A Journal of Integrative Biology, 1*(22), 65–76. https://doi.org/10.1089/omi.2017.0194

[38] Pare, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews.*European Journal of Information Systems 25*(6), 493–508.

[39] Permana, R. I., & Suroso, J. S. (2018). Data governance maturity assessment at pt. xyz.case study: data management division. *International Conference on Information Management and Technology (ICIMTech) Jakarta, Indonesia (IEEE)*, 15–20. https://doi.org/10.1109/ icimtech.2018.852814

[40] Potančok, M. (2019). Role of Data and Intuition in Decision Making Processes. Journal of Systems Integration, 10(3), 31–34. https://doi.org/10.20470/jsi.v10i3.377

[41] Putrus, R. (2019). The Role of the CISO and the Digital Security Landscape. *ISACA Journal, 2019*(2), https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/the-role-of-the-ciso-and-the-digital-security-landscape

[42] Rodríguez-Dorans, E., & Jacobs, P. (2020). Making narrative portraits: a methodological approach to analysing qualitative data.*International Journal of Social Research Methodology, 23*(6), 611-623. https://doi.org/10.1080/13645579.2020.1719609

[43] Singh, N., Krishnaswamy, V., & Zhang, J. Z. (2022).Intellectual structure of cybersecurity research in enterprise information systems.*Enterprise Information Systems,* https://doi.org/10.1080/17517575.2022.2025545

[44] Sools, A. (2020). Back from the future: a narrative approach to study the imagination of personal futures. *International Journal of Social Research Methodology, 23*(4), 451-465. https://doi.org/10.1080/13645579.2020.1719617

[45] Stedman, C., &Vaughan, J. (2022).What is data governance and why does it matter? Retrieved from https://www.techtarget.com/searchdatamanagement/definition/data-governance

[46] St-Hilaire, W. A. (2020). Digital risk governance: Security strategies for the public and private sectors. col. Economics and public administration. *1. Springer International Publishing*. 1–XVIII, 218

[47] St-Hilaire, W. A. (2021). Leading with Digital Technologies Governance in the State-Owned Enterprises.International Journal of Public Administration, 1-14. https://doi.org/10.1080/01900692.2021.1993898

[48] Sun, L., Zhang, H., & Fang, C. (2021). Data security governance in the era of big data: status, challenges, and prospects, *Data Science and Management, 2*(1), 41-44. https://doi.org/10.1016/j.dsm.2021.06.001.

[49] Trom, L., & Cronje, J. (2020). Analysis of data governance implications on big data Future of Information and Communication Conference 14-15 March 2019 1 (Springer, Cham) San Francisco, CA, USA. , 69. https://doi. org/10.1007/978-3-030-12388-8_45

[50] Tziahanas, G., & Novak, K. (2022).Is a Merger between Information Security and Data Governance Imminent? Retrieved from https://www.cpomagazine.com/cyber-security/is-a-merger-between-information-security-and-data-governance-imminent/

[51] Vaibhav, A. V. (2021). Information security governance metrics: a survey and taxonomy, Information Security Journal: *A Global Perspective,*1-13. https://doi.org/10.1080/19393555.2021.1922786

[52] Venkatraman, S., & Venkatraman, R. (2019). Big data security challenges and strategies. AIMS Mathematics, 4(3), 860-879. https://doi.org/10.3934/math.2019.3.860

[53] Wang, Y., Zhao, M., Hu, Y., GAO, Y., & Cui, X. (2021). Secure computation protocols under asymmetric scenarios in enterprise information system, *Enterprise Information Systems, 15*(4), 492-512. https://doi.org/10.1080/17517575.2019.1597387

[54] Zhang, D. (2018). Big Data Security and Privacy Protection.Conference: 8th International Conference on Management and Computer Science (ICMCS 2018). https://doi.org/10.2991/icmcs-18.2018.56

[55] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities,A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.09 564