MedCrave
Step into the World of Research
International Journal of Complementary & Alternative Medicine

Review Article

Open Access
CrossMark

Review of issues on knowledge management system and country's digital security: a study of Nigeria

Abstract

The digital world has exposed the whole world into danger and vulnerability of information security and the presence of new ways of compromising information security has moved the attention to a more holistic approach to information security management comprising technological, organizational, and social components. This remains a challenge for the policy maker and practitioners to more concerted effort into creating secure knowledge management and making the appropriate knowledge accessible to the appropriate individuals at the appropriate time. Knowledge is known as a country intellectual infrastructural and significant to overall development of all sectors.

Keywords: knowledge management, security, technology and nigeria

Volume 16 Issue 2 - 2023

Dauda Adegoke Adejumo
Department of PhD Economics and Business Science, Universidade de Aveiro, Portugal

Correspondence: Dauda Adegoke Adejumo, PhD Economics and Business Science, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal, Email daudaadejum2@ua.pt

Received: Ferbruary 25, 2023 | **Published:** March 06, 2023

Introduction

The interdependence of telecommunications and digital world has exposed the whole world into danger and vulnerability of information security and the presence of new ways of compromising information security has moved the attention to a more holistic approach to information security management comprising technological, organizational, and social components (Kayworth & Whitten, 2010). Digital Security is an act of controlling access to data, information, and knowledge while knowledge management is about getting needed data, information, and knowledge to the right people at the right time. It is correct to say knowledge management and information security are complementary.[1] Knowledge management is also vital to government of all countries because it affects country security (Al Shraah, Abu-Rumman, Madi, Alhammad & AlJboor, 2021). The relevant of knowledge to a country digital security makes it a subject of attacks by criminals within and outside, and it is apparent that most government lack absolute control to handle information security activities because of borderless nature of information. This challenges practitioners to more concerted effort into creating secure knowledge management and making the appropriate knowledge accessible to the appropriate individuals at the appropriate time. Considering the competitive value of data, information, and knowledge to the organizations that own them, it is only natural that organizations would want to take steps to protect these assets. Hence, it requires a holistic information security management approach that emphasizes the importance of taking account of the human factor in organization information security which includes attitudes, beliefs, norms, behavioral patterns, leadership, culture, employee awareness etc.[2] To encourage adherence to related rules and procedures, prior research has underlined the significance of providing information security training to staff Considering the cyber threat environments, government should take a precaution and policy to guide against stolen or attack on their security infrastructure, ensure that unauthorized person has limited access to country information. The strength of every country is determined by its environment security that is more reason why the security personnel need training, awareness, and motivation to be able to protect intellectual property of the country against cyber threats. A country security personnel should manage information sharing on social platforms and protect country´s intellectual properties through a secured environment. Knowledge management (KM) is one of the key factors to foster a secured digital environment and it is about sharing and transferring knowledge from knowledge sources to knowledge users.[3] Knowledge management (KM) provides a formal mechanism for the identification and distribution of knowledge including security information.[4] According to Jouini, Rabaiand Aissa,[5] Knowledge management is the process of creating, sharing, using, and managing the knowledge and information of an organization. It involves capturing, distributing, and effectively using knowledge to support the goals and objectives of the organization. Country digital security is a broad term that refers to the measures that a country takes to secure its digital infrastructure, including its networks, systems, and data. It encompasses a wide range of activities, including cyber security, data protection, and digital privacy. These measures are important for protecting a country's national security, economic prosperity, and social well-being. Peltier,[6] added that information security is about protecting assets, networks, data, information, computers, and applications by restricting access to the assets and preventing unauthorized modification or destruction. The issue of knowledge management has no exception to country's security because of environmental protection and challenges facing sustainable development.[7] As a result, this current study will adapt from the roles knowledge management plays in organizations.[8] It is obvious that the complex environment is significantly increasing due to globalization, technological innovation, climate, and social change which requires more efficient and agile approaches to knowledge creation and management.[8–14]

Knowledge is seeing as intellectual property of any organization or country.[15] As a result, the concept of knowledge management (KM) is one of the corporate sector's fastest-growing subsectors in this period of constantly evolving technology and globalization (Areed et al., 2021). Through individual social ties, suitable corporate culture, and external networks that support the acquisition and absorption of external knowledge, KM processes see knowledge as being created, shared, and applied on digital means. Almost all the processes involved in knowledge management are done virtually and members have created a community. In view of this, it is crucial to have a workplace culture that supports employees' efforts to develop, store, transmit, and apply knowledge.[16] In addition, knowledge resources are used successfully, a variety of advantages can be expected, including quicker decision-making, the avoidance of duplication of work, a faster pace of delivery and customer response, and increased organizational efficiency, effectiveness, and creativity.[16]

The rise in Cybercrime Report on data breeches is exponentially growing and it keeps increasing because the criminals are more advanced on technology while the country personnel's handles

Information management with less skilled Chigada &Madzinga,[17] Data breaches may include credit card numbers, personal identity information, and intellectual property.[18] It is mostly horrible when insiders are involved in web-based attacks and result to cyber espionage. Cyber terrorism is another reason why country information needs to be secured in order not to incite fear through violence or the threat of violence at the direction of a militant belief system. Cyber-terrorism refers to the use of Web-based information technology to carry out enabling, disruptive, or destructive activities in the digital domain.[19] Cyber hackers if gained access to sensitive information and use it to exploit the security infrastructure by exposing the country into risk. A hacker can modify or distort digital data to spread false information or otherwise compromise digitalized control systems, harming or even obliterating crucial infrastructure functions.[20] The Islamist terrorist organizations (al-Qaeda) had spent time to study security information of western and results to their vulnerability,[21] as American investigators found operatives utilizing telecom switches in several nations.[22] Nowadays, a war is won through the concerted ability to secure information not on the physical strength.

Knowledge is important and it is an intellectual property of any organization or country.[15] Ultimately there are persistent threats that are risks to the knowledge relied upon by organizations or country due to technological innovation such as smart phones and tablets have become tools in security management and their simplistic, inexpensive, and ubiquitous make it accessible to track location and identify images by users. Furthermore, some developed countries such as United States and European Unions have grown their sensitivity on the cybersecurity and there is strategy on Indications, publication plans, and directives that govern a safe digital environment for their member States. There is government approach towards training and awareness on Knowledge management whereby the stakeholders will be able to use their experience to secure country information most especially in the era of cyber threat. For instance, Cloud and mobile technologies is a global concern and this requires government sensitivity by always providing a platform for control.

But digital security is still being polarised in most developing countries, especially in Nigeria. The security apparatus indicator considers the security threats to a state, such as bombings, attacks and battle-related deaths, rebel movements, mutinies, coups, or terrorism. The Security apparatus also considers serious criminal factors, such as organized crime and homicides, and perceived trust of citizens in domestic security. The higher the value of the indicator, the more the threats in the state. This situation give rise to cybercrime, cyber espionage, cyber war, and cyber terrorism as a resultant effect of abject poverty, political differences, ethnicity problem, lack of training, awareness, social culture, non-data-base and non- infrastructural policy. The government inability to take security precaution and policy against stolen or attack of the infrastructure have created series of security problem and the country now experiencing various security issues (Boko-Haram, Ipob, Kidnapping, Yahoo etc), and when security of a country is being threatened it has negative influence on the country's economy which is the bases for growth.

The dearth of studies in developing countries on the linkage of IS Security and KM, Information Security technologies, secure communications, and secure storage. In Nigeria, government has to learn from countries that have successful in the adoption of policy communication or security awareness and training programs which are means or mechanisms to increase or maintain information security knowledge between individuals in an organization or country security agencies.

Nigeria: Security threats index

The Security apparatus indicator considers the security threats to a state, such as bombings, attacks and battle-related deaths, rebel movements, mutinies, coups, or terrorism. The Security apparatus also considers serious criminal factors, such as organized crime and homicides, and perceived trust of citizens in domestic security. The higher the value of the indicator, the more the threats in the state.

The information economy presupposes that the productivity and competitiveness of economic entities depend mainly on their ability to generate, process, and effectively apply information based on knowledge.[23] For that indicator, we provide data for Nigeria from 2007 to 2022. The average value for Nigeria during that period was 9.22 index points with a minimum of 8.7 index points in 2020 and a maximum of 9.9 index points in 2015. The latest value from 2022 is 8.9 index points. For comparison, the world average in 2022 based on 177 countries is 5.09 index point (Figure 1 & 2).

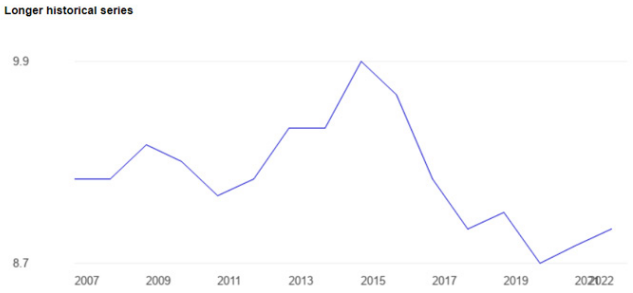

Figure 1 Nigeria economic data from 2007- 2022.

Source: theglobaleconomy.com/ Nigeria

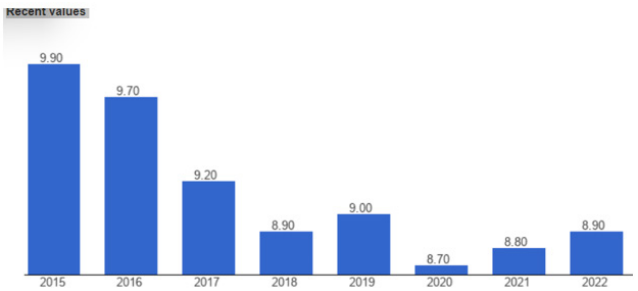

Figure 2 Economics outlook around the world 2015- 2020… **theglobaleconomy.com.**

This suggests need to train stakeholders on Knowledge management to be able to use their experience to secure country information most especially in the era of cyber threat. As the study aims to analyse the contribution of knowledge management to digital security in Nigeria and determining the policy that enhances digital technological innovation to protect security infrastructure through telecommunications**.**

Conceptual review

Knowledge refers to the theoretical or practical understanding of a subject, as well as the information and skills acquired through education or training.[24] Knowledge acquisition, knowledge creation, knowledge documentation, knowledge transfer, knowledge sharing, and knowledge application are the dimensions of knowledge. According to Drucker, knowledge is the only truly valuable resource, particularly in the context of the "post-capitalist" society while land, labor, and money are only secondary resources. The recent studies revealed that public sector organizations should place a higher priority

on serving the residents of the nation than on preserving bureaucracy and favouring political needs.[25] The knowledge-based culture has remained in the competitive and globally connected companies that requires a comprehensive understanding of knowledge usage, sharing, and creation. Additionally, it must be remembered that the advancement of communications and knowledge transmission technologies has contributed to these complications (Bennet and Bennet, 2004). The ability of an organization to produce, capture, utilize, and build organizational and people knowledge and communicate it throughout the company is known as knowledge management (Allameh et al. 2011). The research of Alavi and Leinder (2001) & Chang and Lin (2015), defined knowledge as creation of the sum of the four sub-processes of combination, socialization, externalization, and internalization. Knowledge discovery is represented by combination and socialization (Becerra-Fernandez & Sabherwal, 2015), and knowledge capture is represented by externalization and internalization (Becerra-Fernandez and Sabherwal, 2015).

- Socialization is the process of sharing experiences and thereby creating tacit knowledge such as mental model sand technical skills. Tacit knowledge can be obtained without using language through observation, imitation, and practice.
- Externalization is the process of articulating tacit knowledge in the form of explicit concepts, taking the shapes of metaphors, analogies, concepts, hypotheses, or models.
- Combination is the process of systemizing concepts intoa knowledge system by combining different bodies of explicit knowledge. Explicit knowledge is transferred through media such as documents, meetings, email, and/or phone conversations. Categorization of this knowledge can lead to the generation of new knowledge.
- Internalization is the process of converting explicit knowledge to tacit knowledge and is closely related to learning by doing.

Knowledge management is the process of capturing, distributing, and effectively using knowledge (Hislop, 2016), its goal is to improve decision making, increase efficiency, and foster innovation within an organization. Knowledge management includes processes such as creating and sharing documents and information, knowledge-sharing among team members, and implementing technology to manage and organize knowledge. KM is crucial to organizational improvement and value generation (Massa and Testa, 2009; Abu- Rumman, 2018). KM is a method of producing and distributing information to the appropriate audience at the appropriate time (Bennet and Bennet, 2004). KM can be manipulated and exploited in a way that benefits a company,[26] and strategic process of knowledge results in a decision (Zwain 2012).[27] identified four objectives for knowledge management; create knowledge repositories, improve knowledge access, enhance knowledge environments, and manage knowledge as an asset. Today, organizations and with no exception to countries are facing fierce competition due to globalization and international competition: Therefore, efforts must be made to improve organizational and employees' knowledge in order to cope with this challenge. Digital resources are considered critical success factors for sharing and creating new knowledge. The application of Knowledge management in organization is supported by literatures.[28]

Knowledge management system (KMS) is a technology or set of practices used to identify, create, represent, distribute, and enable adoption of insights and experiences. It is designed to support the collection, organization, maintenance, and dissemination of information within an organization.[29] The goal of a KMS is to support the organization's ability to make effective decisions by ensuring that the knowledge it needs is available when and where it is needed. This can be done through a variety of methods, including databases, document management systems, and collaborative software.

Digital security refers to the protection of digital information and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. It includes a wide range of measures and technologies such as encryption, firewalls, intrusion detection and prevention systems, and access controls. Digital security is important for protecting sensitive information like financial data, personal information, and confidential business information, as well as for maintaining the availability and integrity of digital systems and networks (Kahyaoglu, & Caliyurt, 2018. It also plays a critical role in protecting against cyber threats such as hacking, malware, and phishing. Implementing a strong digital security strategy and regularly reviewing and updating it is crucial for organizations and individuals to maintain the confidentiality, integrity and availability of their digital information and systems.

The interface between a knowledge management system (KMS) and digital security involves ensuring that the information stored in the KMS is secure and protected from unauthorized access, alteration, or destruction.[1] This can be achieved through a combination of technical and organizational measures, such as authentication and access controls, encryption, backups, and regular security audits. Additionally, it is important to have policies and procedures in place to govern the use and handling of sensitive information within the KMS, as well as training for users on security best practices. A well-designed and properly implemented KMS can help an organization to effectively manage and utilize its knowledge, while also protecting it from cyber threats. The stakeholders need to be educated and create awareness on security policies. The National Security Telecommunications and Information System Security Committee model[30] is a standard model used in information security management. The main components of a KMS include secure languages such as security assertion markup languages and secure knowledge query and manipulation language for secure communication; circles of trust where two or more organizations share supplier/customer authentication information (also for secure communication); and digital rights management and secure for access control.[1] Database design to create secure database management systems and addressing the secure storage issue.[31] The access control policies for managing knowledge sharing in virtual KM communities.[32] Jennex & Durcikova[1] proposed a research model investigating the relationships between IS Security components and knowledge. The overall result showed that KM and security are interrelated

Knowledge complexity

According to Li et al.[33] who demonstrated that business-IT governance, operational and business processes, and strategic mechanisms result in a substantial increase in firm performance when they are inter-related with the synergies between managerial, strategic and operational component's part for competition. Davenport and Prusak[26] suggested that a framework for assessing and absorbing new experiences and information is provided by knowledge as an ongoing combination of framed experience, values, contextual information, and expert insight. They discovered that knowledge frequently becomes incorporated in organizational routines, procedures, practices, and norms as well as in artifacts like papers, videos, audio, or repositories. Additionally, they contend that knowledge must incorporate human inputs such as context, culture, experience, and interpretation to be considered valuable.

Citation: Adejumo DA. Review of issues on knowledge management system and country's digital security: a study of Nigeria. *Int J Complement Alt Med.* 2023;16(2):55–62. DOI: 10.15406/ijcam.2023.16.00633

Nonaka and Takeuchi (1995) distinguish between tacit and explicit knowledge. Unstructured information is often thought of as tacit knowledge because it can only be expressed in the knower's mind and cannot be explicitly expressed by data or knowledge representations. Conversely, explicit information, sometimes referred to as organized knowledge that can be directly articulated using knowledge representations. Knowledge is neither fully explicit nor purely tacit instead knowledge is a combination of tacit and explicit information with each user's level of explicitness differing. The end points of this continuum of knowledge are pure tacit and pure explicit, with specific knowledge items occurring somewhere in between. Smolnik et al. (2005) use context explication to adopt a position on the knowledge continuum, where context explication considers the individual's experience and background.

Knowledge transfer

Knowledge transfer in an organization occurs when members of an organization pass knowledge to each other. knowledge sharing will benefit to the business success (Remus, 2012). knowledge is resided in members' minds (Wasko & Faraj, 2000) and the holder of knowledge can decide to participate in knowledge sharing or not (Chiu, Wang, Shih, & Fan, 2011). According to Yuan et.al (2022) who stated that innovation comes from individual creativity, and collective decision contribute to innovation as employees are giving opportunity to share their knowledge and experiences on a particular issue. In this sense, members should be motivated to share their knowledge to sustain the survival of a country through information system (Ridings, Gefen, & Arinze, 2006). Trust and commitment are treated as critical factors that may impact knowledge sharing (Chang, Hsuand, Lee, 2015).

Security as component part of knowledge management

Opinion of some researcher is that security appears a barrier to knowledge security is about protecting something.[34] Information security is about protecting assets such as networks, databases, computers, and applications while Knowledge management (KM) is about sharing and transferring knowledge from knowledge producers to knowledge users. KM can be defined as the capturing of knowledge from past decision-making for application to current decision making with the express purpose of improving organizational performance.[35] Most of recent studies by researchers and practitioners emphasize that security and KM are related.[34] According to Maule (2006), military and government organizations also use KM to support decision making and to create intelligence value and tactical and strategic advantage. Knowledge management project should in security as an integral component and traditional security is reflected with the Technical Resources construct of the System Quality dimension and includes the technical controls needed to protect the basic technical system components of the KMS,[34] The components of this construct include databases, web sites, networks, and other IS components. System Quality refers to how well these components work and for them to work as expected, technical security controls such as firewalls, intrusion detection, cryptography, and access controls are utilized. The fact that this is standard security and not what is being presented as KM Security is emphasized. This is evident in the research conducted by Jennex & Olfman (2005) where 12 critical success factors were identified in support of knowledge management and knowledge management security

a) A Knowledge Strategy that identifies users, sources, processes, storage strategy,

b) Knowledge and links to knowledge for the KMS.

c) Motivation and Commitment of users including incentives and training

d) Integrated Technical Infrastructure including networks, databases/ repositories,

e) computers, software, KMS experts

f) An organizational culture and structure that supports learning and the sharing and use

g) of knowledge

h) A common enterprise-wide knowledge structure that is clearly articulated and easily

i) understood

j) Senior Management support including allocation of resources, leadership, and

k) providing training

l) Learning Organization

m) There is a clear goal and purpose for the KMS

n) Measures are established to assess the impacts of the KMS and the use of knowledge

o) as well as verifying that the right knowledge is being captured

p) The search, retrieval, and visualization functions of the KMS support easy knowledge

q) use

r) Work processes are designed that incorporate knowledge capture and use

s) Security/protection of knowledge

KM security

According to current theories of information security management, security is a task that integrates managerial, organizational, and technical concerns into a strategy for managing organizational risk. Security encompasses all administrative, managerial, and technical controls which includes a thorough plan outlining the organization's security implementation procedures, training, and awareness campaigns.[36] The recent studies have emphasized incorporation of security into KM success which forms the basis for KMS design. So, by creating secure KMS it will increase the ability of all organizations, business, government, or military, to improve the transfer of knowledge to key decision makers. This will lead to increased organizational performance which supposed to be the primary goal of KM.

Among the requirements for knowledge is that managers understand the structures and processes within the organization and how to engage with external partners.[25] A common model used in information security management is the National Security Telecommunications and Information System Security Committee model.[30] This is a thorough model for creating a security strategy to safeguard information systems and can be applied to any organization without being impacted by organizational differences because it does not incorporate any specific organizational needs or characteristics.[37] It is independent of technology because it does not specify any specific technologies, only the functions that technologies perform, and emphasis on safeguarding storage, processing, and transmission assets. When this is used for knowledge management, the emphasis is on safeguarding knowledge repositories and knowledge mnemonic

functions (search, retrieve, compare, etc.) are employed in knowledge processing, knowledge manipulation, and communication processes for knowledge transfer. It also highlights the necessity of safeguarding the availability, confidentiality, and integrity of data.

Traditional security is portrayed with the Technical Resources construct of the System Quality dimension, which also incorporates the technical controls required to safeguard the KMS's fundamental technical system components. Networks, databases, websites, and other elements of the IS make up this construct. Technical security measures like firewalls, intrusion detection, cryptography, and access restrictions are used to ensure that these components perform as expected, which is referred to as system quality (Figure 3).[38]

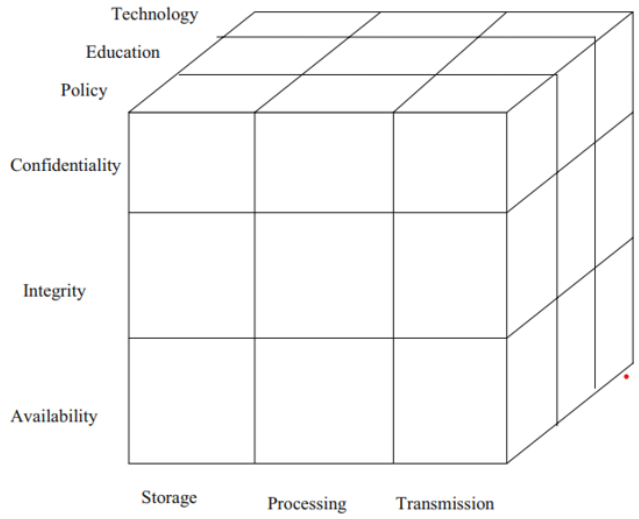

Figure 3 NSTISSC security infrastructure model (NSTISSC 1994, p. 18).

Telecommunications

The mobile technological tools use in the transmission of information over distance. Research have identified challenges as telecom market continue to launch new applications such as sensors, cameras, Global Positioning System (GPS) and other in-built components introduce many new services (Callanan, Jerman-Blažič & Blažič, 2016). However, they can give rise to fresh difficulties including data protection weaknesses and breaches of user privacy. Users typically expect a mobile device's underlying framework to be safe or sufficiently alert to warn them of any potential threats from malware incursion or an interception tool that has been accidentally introduced by network operators or is included in a downloaded mobile phone application.

Privacy

Privacy concerns have been a controversial issue long before the beginning of the information technology era. However, privacy concerns have been highlighted as a major challenge for the digital world. Previous research has recognized that personal data privacy is an issue of growing significance, particularly in online contexts. Indeed, the open nature of Internet-enabled systems has been responsible for a considerable erosion in privacy-related matters. Privacy concerns have become a more alarming, challenging, and problematic issue in information security because online activities are not properly regulated in some developing countries. This strategy (European Commission, 2013) clarifies the principles that the European Union intends to follow regarding cyber security policy within the Union and internationally. Through this document, the European Commission (EC) aims to tackle crucial challenges such as protecting fundamental rights, freedom of expression, personal data and privacy, guaranteeing the Internet's integrity and security to allow safe access for all, supporting a multi-stakeholders governance approach, generate awareness on the shared responsibilities public authorities, private sector and individual citizens have to take action to protect themselves, and ensure a coordinated response to strengthen cyber security. Several strategic priorities and actions that can enhance the EU's overall performance are identified within the strategy.

Social and cultural theory

Crossler et al. (2013) argues that national culture likely has a direct impact on various elements of information security and suggested that cross-cultural differences need information security. In a multi-cultural environment, for instance, a less individualist culture may therefore lead to organizational members being more loyal to their organization than they would in a nation where an individualist culture is more predominant (Boyacigiller & Adler, 1991).So, also concept of social influence (social norms)is a prominent indicator on intention behaviour to the adoption of new technology by the theory of reasoned action, and thus refers to the individual's perception that most people who are important to him think he should or should not perform the behaviour in question.[28] The aspect of social norms has been generally linked to the adoption dynamics of different digitized and non-digitized technologies because of their influence in shaping human behaviour and perceptions.[39] Consequently, social norms have been acknowledged as a primary component in affecting users' behaviour towards technology acceptance and use. From the perspective of the social norms are defined as the degree to which a user believes that other people expect him or her to use a specific. Some people may come into the believe that GPS exposes them to no confidentiality despite its advantage on environmental safety and make life easier to live.

Perceived image and political ideology

The issue of image in technological innovations have become relevant and now use for social status and prestige by organization, institution, and country. Thus, user-image perceptions could be considered as a primary social factor that effectively drives the acceptance and adoption ofa specific innovation.[39] Several studies have confirmed that perceptions of image play a critical role in enhancing the adoption dynamics of various IT domains in developing countries. The image was initially introduced to the IT adoption research by Moore and Benbasat[40] where he defined image as "the degree an individual perceives that the use of innovation will boost his or her image and will achieve a higher social status in society," recognizing the importance of individual-image perceptions in influencing behavioural intention to adopt information technology innovation. The growing in political differences create a barrier in policy formulation. Party members try to move against any view that is not coming from his / her camp and slow down decision of the government. A reflection of nation image is her political activities and when the political circle is in crisis, the nation tends to have negative image.[41]

Perceived physical risk

Technology adoption literature has long considered the risk of using technology, particularly physical risk. The new wave of emerging pervasive applications has a health-risk behaviour, especially those applications that are driven by technologies. To understand how they affect the relationships between a few factors related to technology adoption processes and behavioural intention, the study has identified

the effects of all types of risks associated with recently introduced IT products and services. The perceived physical risk is no exception. Undoubtedly, the degree of linkages between elements influencing how emerging technologies are adopted and accepted and behavioural intention are sensitive to the perceived danger that potential adopters are willing to accept (high versus low perceived physical risk). Understanding what elements support or undermine a relationship with behavioral intention is made possible by the moderation perspective. The rumour of health risk by long time sitting in a car with GPS has not been substantiate by any study.

Citizen engagement in digital trust

The conviction that technology, people, and processes interact or work together to meet people's digital expectations, including a sense of security, confidence, or control to assist the development of a secure digital environment. In today international practice, it is central to any organization/firm's success to embrace technology culture as basis for trust.[42] Therefore, digital trust is crucial into the environment of an organization, especially for establishing and maintaining connections with all stakeholders. The government of developed countries have been able to improve digital security by Citizen involvement in the activities such as private detective. In sum, citizen involvement can allow the police to leverage their assets by tapping into the knowledge, the resources, and the abilities of organisations and individuals outside of law enforcement' while 'working with communities to build trust, legitimacy, and accountability'. According to Gupta et al. (2012), relational and transactional psychological contracts positively affect knowledge contribution with an organization. This confirms that individual behaviour in a virtual community depends on trust and collaboration about knowledge sharing.

Empirical study of knowledge management and country digital security

Elaswad & Jensen[43]''Introducing E-Government in developing countries analysis of Egyptian e-Government services,'' the study revealed that developing countries, needs to identify citizen's requirements as well as the technology and digital infrastructure to resist cybercrimes which has not previously existed in their society. According to the work of Lin, Liu, Li, Zhang, & Ji,[7]''Construction of Digital Mine and Key Technologies'' opined that the digitalization of all important spatial data and attribute data, including mine building, exploration, development, mining, environmental protection and control, is made possible by computers and network connectivity. In the study of Nasser (2020) ''CYBERCRIME: THEORETICAL DETERMINANTS, CRIMINAL POLICIES, PREVENTION & CONTROL MECHANISMS'' revealed that education is perceived to be one of the most effective measures to promote digital security and new block chain technologies allow for taking preventive measures and improving the protection of sensitive information. Jennex & Zyngier.[34] Security as a contributor to knowledge management success'' suggests application of security technology in KM, as well called for extension of the KM security to other disciplines such as risk management in KM strategy, KM management/governance support, and to improve the value of knowledge.[44–55]

This study deduced from above positions that it is important that Nigerian government take serious measures on data protection especially in this era of digitalization as it contributes greatly to posterity of a nation.

Conclusions

Most of the previous studies focused on organization but since there is relevant in roles of organization in nation. The security of knowledge objects employed in knowledge management is not sufficiently developed, according to the paper's findings. Information security standards and regulations within the firm must be integrated into knowledge management governance. Practitioners of KM must collaborate with practitioners of information security, and moreover, digital security is a responsibility of all citizens of the country in respectful of organization, party, ethnic, religion, belief, culture etc. There is need for partnership of the Nigerian IT security experts with software engineers on innovations like cloud and mobile technologies to enhancing country's' capacity to gather and make knowledge accessible to those in need. However, government must strike a balance between safeguards that guarantee that only those who are permitted are accessing that knowledge and ease and speed of knowledge exchange. Many KM researchers also concentrate on figuring out and removing obstacles to knowledge transmission and sharing. These same researchers must understand how to obtain information security controls, ensuring that removing obstacles to knowledge transfer and sharing do not render necessary access control schemes ineffective or make it more challenging to develop and implement an access control paradigm on what is typically regarded as a crucial organizational asset. In the end, this study concludes that while Information Security and Knowledge Management must be integrated, neither scholars nor practitioners are making enough effort to do so. Hence, there is need for further study on the use of blockchain and Facial ID technology that can monitor and help to curb cyber-attacks.

Suggestion for future research

This paper wishes to suggest further investigation into the methods of technological innovation that can be adapted for the country digital security measure such as Facial Identification technology that can easily detect the face of cyber attackers. In addition, there is need to improve on framework of Knowledge management and country digital security because most of existing literature focus on organizations.

Acknowledgements

None.

Conflicts of interest

We declare there are no conflicts of interest.

Funding

None.

References

1. Jennex M, Durcikova A. Integrating IS security with knowledge management: Are we doing enough?International *Journal of Knowledge Management (IJKM)*. 2014;10(2):1–12.
2. Rocha Flores W, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers and Security*. 2014;43:90–110.
3. Dehghani R, Ramsin R. Methodologies for developing knowledge management systems: an evaluation framework. *Journal of Knowledge Management*. 2015;19(4):682–710.
4. Abdullah H, Uli J, Mohamed ZA. Relationship Between Organizational Characteristics and Information Security Knowledge Management Implementation. *Procedia–Social and Behavioral Sciences*. 2014;123:433–443.
5. Jouini M, Rabai LBA, Aissa AB. Classification of security threats in information systems. *Procedia Computer Science*. 2014;32:489–496.

6. Peltier TR. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. USA: CRC Press; 2016.
7. Lin H, Liu P, Li W, et al. Construction of digital mine and key technologies. *In Advanced Materials Research*. 2012;524:413–420.
8. Nissan E, Galindo Martín MÁ, Méndez Picazo MT. Relationship between organizations, institutions, entrepreneurship and economic growth process. *International Entrepreneurship and Management Journal*. 2011;7(3):311–324.
9. Merritt TP. Forecasting the future business environment – the state of the art. *Long Range Planning*. 1974;3(2):54–62.
10. Chakravarthy B. A new strategy framework for coping with turbulence. USA: Sloan Management Review, Winter; 1997. pp. 69–82.
11. Weber Y, Tarba SY. Strategic agility: a state of the art. *California Management Review*. 2014;56(3):5–12.
12. Soto–Acosta P, Cegarra–Navarro JG. New ICTs for knowledge management in Organizations. *Journal of Knowledge Management*. 2016;20(3):417–422.
13. Soto–Acosta P, Popa S, Martinez–Conesa I. Information technology, knowledge management and environmental dynamism as drivers of innovation ambidexterity: a study in SMEs. *Journal of Knowledge Management*. 2018;22(4):931–948.
14. Shams SR, Vrontis D, Weber Y, et al. Cross–Functional Knowledge Management: The International Landscape. USA: Routledge Taylors and Francis Group; 2019. P. 236.
15. Dosi G, Stiglitz JE. The role of intellectual property rights in the development process, with some lessons from developed countries: an introduction. *Intellectual property rights: Legal and economic challenges for development*. 2013;1:1–55.
16. Chang CM, Hsu MH, Lee YJ. Factors influencing knowledge–sharing behavior in virtual communities: a longitudinal investigation. *Information Systems Management*. 2015;32(4):331–340.
17. Chigada J, Madzinga R. Cyberattacks and threats during COVID–19: A systematic literature review. *South African Journal of Information Management*. 2021;23(1):1–11.
18. Poyraz OI, Bouazzaoui S, Keskin O, et al. Cyber–assets at risk (CAR): The cost of personally identifiable information data breaches. In ICCWS 2020 15th international conference on cyber warfare and security. USA: Academic Conferences and publishing limited; 2020.
19. Zuberi KJ. Use of cyber space by terrorist organizations. *International Journal for Electronic Crime Investigation*. 2018;2(1):6–6.
20. Vähäkainu P, Lehto M, Kariluoto A. Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures. Springer, Cham: In Cyber Security: 2022. pp. 255–292.
21. Byman D. Buddies or burdens? Understanding the Al Qaeda relationship with its affiliate organizations. *Security Studies*. 2014;23(3):431–470.
22. Benson. DC. Why the internet is not increasing terrorism. *Security Studies*. 2014;23(2):293–328.
23. http://nbuv.gov.ua/UJRN/Vsuem_2013_1_5
24. Pritchard A. Ways of learning: Learning theories for the classroom. UK: Routledge; 2017.
25. Del Giudice M, Carayannis EG, Maggioni V. Global knowledge intensive enterprises and international technology transfer: emerging perspectives from a quadruple helix environment. *The Journal of Technology Transfer*. 2017;42(2):229–235.
26. Davenport, D. L., &Holsapple, C. (2006). Knowledge organizations (encyclopedia of knowledge management)
27. Robinson HS, Carrillo PM, Anumba CJ, et al. Perceptions and barriers in implementing knowledge management strategies in large construction organisations. *In Proceedings of the RICS COBRA Conference*. 2002. pp. 451–46.
28. Ajzen I. The theory of planned behavior: Frequently asked questions. *Hum Behav Emerg Tech*. 2020;2(4):314–324.
29. Santoro G, Vrontis D, Thrassou A, et al. The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity. *Technological Forecasting and Social Change*. 2018;136:347–354.
30. Ferris M. New email security infrastructure. In Proceedings of the 1994 workshop on New security paradigms. 1994. pp. 20–27.
31. Moura J, Serrão C. Security and privacy issues of big data. In *Handbook of research on trends and future directions in big data and web intelligence*. USA: IGI Global; 2015. pp. 20–52.
32. Rao M. *Knowledge management tools and techniques*. UK: Routledge; 2012.
33. Li W, Liu K, Belitski M, et al. e–Leadership through strategic alignment: an empirical study of small–and medium–sized enterprises in the digital age. *Journal of Information Technology*. 2016;31(2):185–206.
34. Jennex ME, Zyngier S. Security as a contributor to knowledge management success. *Information Systems Frontiers*. 2007;9(5):493–504.
35. Jenner ME, Olfman L. A model of knowledge management success. *International Journal of Knowledge Management (IJKM)*. 2006;2(3):51–68.
36. Talbot J, Jakeman M. Security risk management body of knowledge. USA: John Wiley & Sons. 2011. p. 480.
37. Crowley E. Information system security curricula development. In Proceedings of the 4th Conference on Information technology curriculum. 2003. pp. 249–255.
38. Pearce M, Zeadally S, Hunt R. Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*. 2013;45(2):1–39.
39. Faqih KM. Factors influencing the behavioral intention to adopt a technological innovation from a developing country context: The case of mobile augmented reality games. *Technology in Society*. 2022;69:101958.
40. Moore GC, Benbasat I. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*. 1991;2(3):192–222.
41. Fayomi OO, Chidozie FC, Ajayi LA. Nigeria's national image and her foreign policy: An exploratory approach. *Open Journal of Political Science*/ 2015;5(3):180.
42. Parsons KM, Young E, Butavicius MA, et al. The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*. 2015;9(2):117–129.
43. Elaswad O, Jensen CD. Introducing E–Government in developing countries analysis of Egyptian e–Government services. USA: IEEE, In 2016 IST–Africa Week Conference; 2016. pp. 1–13.
44. Abdullah H, Uli J, Mohamed ZA. Relationship Between Organizational Characteristics and Information Security Knowledge Management Implementation. *Procedia–Social and Behavioral Sciences*. 2014;123:433–443.
45. Al Shraah A, Abu–Rumman A, Al Madi F, et al. The impact of quality management practices on knowledge management processes: a study of a social security corporation in Jordan. *The TQM Journal*. 2021;34:4.

Citation: Adejumo DA. Review of issues on knowledge management system and country's digital security: a study of Nigeria. *Int J Complement Alt Med.* 2023;16(2):55–62. DOI: 10.15406/ijcam.2023.16.00633

46. Dehghani R, Ramsin R. Methodologies for developing knowledge management systems: an evaluation framework. *Journal of Knowledge Management*. 2015;19(4):682–710.

47. Hislop D. Knowledge management. In: Encyclopedia of human resource management. UK: Edward Elgar Publishing Limited. 2016.

48. Jouini M, Rabai LBA, Aissa AB. Classification of security threats in information systems. *Procedia Computer Science*. 2014;32:489–496.

49. Kahyaoglu SB, Caliyurt K. Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*. 2018;33(4).

50. Nasser AL. Cybercrime: Theoretical Determinants, Criminal Policies, Prevention & Control Mechanisms. *International Journal of Technology and Systems*. 2020;5(1):34–63.

51. Peltier TR. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. USA: CRC Press; 2016.

52. Rocha Flores W, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers and Security*. 2014;43:90–110.

53. Sherif K, Sherif SA. Think social capital before you think knowledge transfer. *International Journal of Knowledge Management (IJKM)*. 2006;2(3):21–32.

54. Wah CY, Menkhoff T, Loh B, et al. Social capital and knowledge sharing in knowledge–based organizations: An empirical study. *International Journal of Knowledge Management (IJKM)*. 2007;3(1):29–48.

55. www.theglobaleconomy.com

Citation: Adejumo DA. Review of issues on knowledge management system and country's digital security: a study of Nigeria. *Int J Complement Alt Med.* 2023;16(2):55–62. DOI: 10.15406/ijcam.2023.16.00633