Peace Studies and Practice
Journal of the Society of Peace Studies and Practice

Volume 14 | Issue 1 | August 2026
Pp 1 - 14

Co-creating Community Peace: Leveraging on Information Security Management in Oyo State, Nigeria

[1] OLADIPO, Oladapo David
[2] ALUKO, Benjamin Adeniran
DOI: https://doi.org/10.63725/jpsp.v14i1.01

Abstract

Sustainable peace has never been so much a desired commodity in Nigeria's nationhood journey as it is today. The fragility of Nigeria's socio-political landscape, the attendant economic woes, corruption, and protracted insecurity with its hydra-headed manifestations through religion and ethnicity from the North to the South make sustainable peace a priceless commodity. To achieve peace without co-creating peace with the host community may be challenging. The study investigated the deployment of Information Security Management and Co-creating Community Strategy for Peace in Ibadan North Local Government Area of Oyo State. The study was anchored on Risk Management theory of information security. However, this theory was developed in the 1970s by the psychologists Amos Tversky, Daniel Kahneman, and Paul Slovic. From the investigation they carried out, an important aspect of information security and risk management is recognising the value of information and defining appropriate procedures and protection requirements for the information. A descriptive research design was adopted for the study through a quantitative method with the use of questionnaires. The purpose of using descriptive research is to determine the situation as it existed at the period of study. Primary and secondary method of data collection was used. More so, the study population comprised all personnel of Ibadan North Local Government Area of Oyo State, which includes male and female senior personnel. Total number of eighty (80) questionnaires were administered, while 78 were correctly filled and returned, on which the analysis depended. The study reveals that Ibadan North LGA is trying possible means to inculcate the use of ISM, such as having an ICT, tracking, and intelligence-gathering department. Likewise, availability of necessary equipment such as CCTV, surveillance cameras, GPS, Drones, Motion sensors and Alarm systems for their security unit. However, there are various challenges in using ISM such as lack of fund, unwillingness of some staff to give detail information on security issues among others. Conclusively, information security management should be seen as strategy rather than merely operational routine. The gathering of information must not be taken for security protection itself. It must be processed, analysed and managed for sound intelligence sharing and decision making. Overhauling of security equipment for timely, effective and efficient communication is key to safety and management. Working with outdated tools and equipment can compromise information security.

[1&2] Department of Peace, Security, and Humanitarian Studies
Faculty of Multidisciplinary Studies
University of Ibadan, Nigeria

Keywords: Co-creating, Community Peace, and Information Security management

Introduction

In any society that lives together as a group, security problems become inevitable. Security of life and property has become a very important issue to contend with in every society. It has become a necessity in every human society and its absence pose danger to the survival of individuals and their properties. Apparently, no state can claim to give one hundred percent safety for her populace; hence, no society is devoid of crime and insecurity (Iyang and Abraham, 2014). Daily reports on criminal activities by various security agencies around the world show that crime is a marvel that cannot be eradicated from any society. In fact, Durkheim, as one of the founding fathers of Sociology, was of the view that crime is normal and functional to the society. Consequently, various means of containing and managing security to attain the lowest possible crime rate with optimum resource spending have been developed by state governments around the world and Nigeria.

Crime and insecurity remain the largest danger to humanity in Nigeria because many people no longer sleep with their eyes closed. Criminal acts like kidnappings, armed robbery, corruption, terrorism, cybercrimes, conflicts, pipe vandalism to mention but a few, have become the order of the day (Bamidele, Akintola and Nuhu, 2016). As such, it is safe to say that Nigeria is no longer a secured society. To minimise the rate of crime and ensuring safety and security in the society, different measures like man guarding an access control, the installation of surveillance cameras in public places, guards patrolling have been put in place (Dambazau, 2008).

There seems no contention regarding the strategic relevance that security holds in the development of any nation. Certainly, security of lives and property remains paramount to the evolution of state. This view finds its inspiration in the intellectual conception of Thomas Hobbes through his work on social contract painting a gory picture of the affairs of men in the state of nature where there was manifestly an absence of government to regulate relationships among men. The ruthless and disorderly nature of the Hobbesian state compelled people to rise in unison and decide to surrender their individual powers to a central authority from whom they believed that their security and wellbeing could be actualised. Security can simply be defined as "freedom from danger, that is, protection from physical or direct violence, and freedom from fear that is, a sense of safety and relative wellbeing in political, legal, socio-economic and cultural terms, that is, a measure of protection from structural violence" (Wairagu, Kamenju and Singo, 2004).

Undoubtedly, the issue of security remains important to the continued socio-economic survival of any people (Hyden, 1995). It is for this reason that there have been different efforts by stakeholders especially governments to develop frameworks to advance security of their people and develop strategies to mitigate the risks that both human and non-human threats can pose to the wellbeing of the people. One of such efforts in human history was the conception of the modern state crafted to enjoy all sorts of privileges and rights such as civil obedience as it is also expected to reciprocate such civil gestures of the people by providing them some protection against

DOI: https://doi.org/10.63725/jpsp.v14i1.01

various kinds of internal or external threats (Tilly, 1987).

National security is a premise for national economic growth and development of nations. This is because peaceful nations attract foreign investors while the domestic investors freely operate the economy with little or no tensions and apprehensions. According to Nwanegbo and Odigbo (2013), security is the pillar upon which every meaningful development could be achieved and sustained. In a broad sense, security connotes freedom from, or elimination of, threat not only to the physical existence of the state, but also due to its ability for self-protection and development and the enhancement of the general well-being of the people. On the other hand, information management in the security realm entails the practice of collecting, monitoring and analysing security-related data. It describes "controls that needs to be implemented in order to ensure that it is sensibly protecting the confidentiality, availability and integrity of national and local assets such as citizens, data, borders, economy, etc. from threats and vulnerabilities.

The unavoidable diffusion of security strategies has created concerns about the possibility of information reaching irresponsible hand. In these technology-driven times, the types of issues that threaten national security have shifted dramatically. The problem is reflective in religion, political, economic, social and cultural realities. Information security tools have formed a vital component of national security strategies for controlling proliferation and denying technological advantages to adversaries. However, information security management require the use of technology (tangible and intangible) to identify, generate, process and store information for eventual retrieval and dissemination for use by agencies that require such data for attaining their objectives. These include profiling of perpetrators of crimes and criminalities on land, sea, and air.

Prior to early 21st century, the main objective of information security was to identify the potential risks and threats in critical business processes (Rok and Borka, 2008), protect the financial resources (Raymond, 1990; Yang *et al*., 2005) as well as business reputation, and strengthen the internal compliance with regulations (Qing, Tamara, Paul and Donna, 2002; Basie, 2005). With the continuous improvement of IT and expanded globalised business, today's in-formation security is surrounded by a variety of topics such as Internet of Things (IoT), cloud computing, social engineering, bring-your-own-device (BYOD), threats intelligence programmes and so on. The increased complexity of computer science and expanded scope and scale of information security require companies to obtain a comprehensive understanding about the critical cyber security issues, problems and challenges in order to explore and mitigate their vulnerabilities and effectively protect their confidential data and valuable information assets in this digitalised world. Therefore, this study seeks to examine information security management in IBADAN NORTH AREA, Oyo State.

Community Collaboration/Co-creation

Collaboration is the pooling of resources (e.g., information, money, labour), by two or more stakeholders or partners, to solve a set of problems, which neither can solve individually (Gray, 1985). It involves an interactive process whereby organisations, using shared rules, norms, and structures, act or decide on issues related to a problem

DOI: https://doi.org/10.63725/jpsp.v14i1.01

domain (Wood and Wood, 1991). The intentional goal-oriented collaborative arrangement that emerges is that of a network (Poyhonen and Smedlund, 2004). "Co-creating community peace" refers to a collaborative, bottom-up process where community members, local leaders, and external partners work together to develop context-specific solutions for lasting harmony and stability. This approach emphasises shared ownership, dialogue, and addressing root causes of conflict, rather than imposing top-down solutions.

Key Principles of Co-creating Community Peace

Effective peacebuilding in communities is built on several core principles:

Addressing Root Causes: Sustainable peace requires focusing on underlying issues such as inequality, injustice, lack of economic opportunity, and corruption, rather than just the symptoms of conflict.

Celebrating Diversity and Inclusion: Embracing cultural and social diversity and actively engaging with people from different backgrounds helps to bridge divides and reduce stereotypes.

Collaborative Action and Partnerships: Building peace involves collaboration among community members, local organisations, government, and other stakeholders to leverage resources and implement integrated solutions.

Community Ownership and Alignment: Initiatives must align with the specific needs, strengths, and history of the local community, ensuring local voices and wisdom guide the vision and actions.

Continuous Learning and Adaptation: Peacebuilding is an iterative process that requires ongoing monitoring, evaluation, and adaptation to changing community dynamics and needs.

Inclusive Dialogue and Empathy: Fostering mutual understanding requires open communication, active listening, and empathy, creating a safe space for diverse groups to share their experiences and views.

Transformative Learning: The process itself can foster transformative learning, allowing participants to develop new skills, shift perspectives, and create new, more peaceful narratives.

Practical Activities and Initiatives

Communities can co-create peace through a variety of practical initiatives:

Community Gardens and Shared Spaces: Creating shared physical spaces where people can work together on common goals, such as food security or environmental regeneration, fosters unity and cooperation.

Creative and Arts-based Projects: Collaborative art projects, music events, or theatre can provide a powerful medium for healing, expression, and building trust.

Education and Skills Training: Programmes that teach conflict resolution, critical thinking, and tolerance equip individuals with the skills needed to navigate disputes peacefully.

Interfaith and Inter-generational Dialogues: Events that bring together people from different religious, cultural, or age groups to engage in meaningful conversations and build bridges of understanding.

Promoting Positive Narratives: Utilising media and community platforms to counter

DOI: https://doi.org/10.63725/jpsp.v14i1.01

misinformation and hate speech, promoting positive stories of coexistence and collaboration.

Youth Engagement: Empowering young citizens to take an active role in community development and peacebuilding efforts is crucial for long-term stability.

By applying these principles and engaging in collaborative efforts, communities can move beyond the mere absence of conflict to a state of positive peace, characterised by social cohesion, equity, and stability.

Concept of Peace

The concept of peace has gathered various opinions at various times. However, a seemingly very popular opinion of peace is that it is the absence of war, fear, conflict, anxiety, suffering and violence (Igbuzor, 2010). This perception has been criticised for not being able to create a critical understanding for the meaning and nature of peace. Considering this deficiency, Galtung (2011) attempted to provide a clear definition of the concept and in the process, he distinguished three types of violence that can help to understand the concept of peace. These are: issues of direct violence, structural violence and cultural violence. Direct violence is manifested by physical, emotional and psychological violence, structural violence on the other hand is in the form of deliberate policies and structures that cause human suffering, death and harm while cultural violence involves cultural norms and practices that create discrimination, injustice and human suffering. Galtung also outlined two dimensions of peace. The first is what he called "negative peace" which he described as the absence of direct violence, war, fear and conflict at individual, national, regional and international levels and the positive peace, which he referred to as the absence of unjust structures, unequal relationships, justice and inner peace at individual levels. This definition implies that the concept of peace goes beyond the absence of war, fear, anxiety, suffering and violence as was initially conceived.

In like manner, Ibeanu (2006) approached the concept of peace from the angle of development. He maintains that peace refers to activities that are directly or indirectly linked to increasing development and reducing conflict, both within specific societies and the wider international community. This definition introduces philosophical, sociological and political dimensions of peace and implies that peace is not necessarily a state but a process that involves all steps and machinery that is directed at developing both the human person and the community in which he lives. Politically, however, Ibeanu (2006) explained that peace entails political order. That is, the institutionalisation of political structures in a way that makes justice possible. Thus, he argued that it would be wrong to classify a country experiencing pervasive structural violence as peaceful. This holistic approach to the concept of peace indicates that it is possible for a nation not to be at war and yet not be in peace. In other words, though war may not be going on in a country, the presence of pervasive poverty, oppression of the poor by the rich, police brutality, intimidation of ordinary citizens by those in power, oppression of women or monopolisation of resources and power by some social cleavages in the society or nation, still sends a strong notion that there is no peace in such a nation. Therefore, for any nation to talk about peace, the primary process of creating structures that will ensure justice and welfare of the citizenry must be put in place. Peace is seen as an original, God-given state

DOI: https://doi.org/10.63725/jpsp.v14i1.01

of human existence for men and women. It refers to a state of harmony among people of various standings in which there are no social antagonisms.

Information Security Management

According to the perspective of Pattinson (2007), "an information security management system (ISMS) focuses on managing information security within an organisation, a subject that is of developing concern to many organisations as they deal with the challenges presented in the information society. These challenges include: evolving information security and privacy legislation, published guidelines (Organisation for Economic Cooperation and Development (OECD), Cyber security), and natural threats (fire, flood, earthquake, tornados) or human threats (viruses, spam, privacy, hacking, industrial espionage)". In Information Security Management Systems (ISMS), the information protected goes beyond that residing in electronic formats on computers or networks, but includes paper-based information and extends to intellectual property. In the same year, Pattinson wrote a paper to thoroughly investigate the pith of ISMS. He observed that "by using ISMS an organisation can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs". If they draw from a standardised ISMS framework they can be sure that they are drawing from the experience of many others and that the system has been reviewed and reflects best practices. Such a framework is a tried and tested tool that helps management ensure that security-resource is spent on the most effective areas for the business (Pattinson, 2007).

According to Eloff and Solms (2000), the aim of information security is to protect the information systems and establishes a framework by which organisation can run information systems operation as they are expected. Information security management focuses in minimising the risks of information systems in the operation. There are number of steps included: first, a planning phase allows company to set up security objectives, identify the assets to be protected and choose the framework for implementation; second, implementation phase al-lows the plan to be implemented. During this step, risk assessment and mitigation, training employees about security issues as well as assessment and audit are constantly conducted. Finally, security management should be an ongoing procedure. Managers, IT functions and employees should be constantly aware of security issues and maintain this process to achieve a long-term benefit.

Peltier (2005) provided key qualitative insights with a systems approach toward the humanistic side of information security. The research firmly presents two realms of information security: one lies in the humanistic communication of individuals and the other in information transactions over the computer (virtual). Peltier urges that an effective information security programme cannot be implemented without the implementation of an employee awareness and training programme that addresses the policy, procedures, and tools, so that each individual may understand and utilise.

Moreover, Carlson, Tipton and Krause (2008) characterise information security management systems as "coordinated activities to direct and control the preservation of confidentiality, integrity, and

DOI: https://doi.org/10.63725/jpsp.v14i1.01

availability of information". He notes the concept of ISMS thus: "ISMS is an example of applying the management system conceptual model to the discipline of Information Security". Unique attributes of this instance of a management system include:

a. Risk management applied to information and based upon metrics of confidentiality, integrity, and availability.

b. Total Quality Management (TQM) applied to information.

The Principles of Information Security

The principle of information security are fundamental concept and guidelines that help organisations protect their information assets. Some of which include Confidentiality, Integrity and Availability (CIA) also known as The Information Security Triad. It offers many areas for specialisation including: security network(s) and allied infrastructure, securing applications and databases, security testing, cybersecurity information systems auditing, business continuity planning and digital forensics science, and allied fields.

Donn Parker (2002) proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals. Confidentiality is the term used to prevent the disclosure of information to unauthorised individuals or systems. For example, a credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorised party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in database, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security system typically provides message integrity in addition to data confidentiality. For any information system to serve its purpose, the information must be available when needed. This means that the computing systems used to store and process the information, the security control used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. In

DOI: https://doi.org/10.63725/jpsp.v14i1.01

computing, e-Business and information security it is necessary to ensure that the data, transactions, communication or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are. In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

However, Anderson (2003) points out that the C-I-A triad is just the be-ginning of information security. To extend the principles, he suggests some additional properties such as authenticity, accountability, non-repudiation and reliability. He provides a new definition of enterprise information security which is also called "A well-informed sense of assurance that information risks and controls are in balance". This definition fills the gap which ignored by other definitions and shed light on the importance of governance and management for achieving the security of ISs.

The Concept of Insecurity

Insecurity is the security lapses that continually put the people into tension and the feeling of being unsafe in a particular environment. Beland (2005) posits that insecurity is "the state of fear or anxiety stemming from a concrete or alleged lack of protection." It refers to lack or inadequate freedom from danger. This definition reflects physical insecurity which is the most visible form of insecurity, and it feeds into many other forms of insecurity such as economic security and social security. According to Onifade, Imhonopi and Urim (2013) the level of insecurity in Nigeria country has struck at the fabrics of the country forcing ethnic groups to agitate for the restructuring of the country. Egwu (2001) also claims that the prehistoric tendencies of numerous ethnic groups to resort to violence and religious fundamentalism has intensified the size and propensity of the insecurity, as well as its spread and the scope of its complications.

Origin and Causes of Insecurity in Nigeria

According to Ali (2013) the fear of insecurity in Nigeria is on the increase and this has been compounded by the rising waves of terrorism since the country returned to democratic rule in 1999. Violent crime has a root and history in Nigeria, and could be traced back to the period from 1960 to 1970. At independence in 1960 a federal structure was imposed on Nigeria by the British. Wheare (1963) conceptualises federalism as a constitutional division of power between two levels of government which are independent and coordinating in their respective spheres of influence. Unfortunately, the federal structure bequeathed to Nigeria at independence did not conform to Wheare's tenets of federalism as a system of government where two levels of government exist each sovereign in its sphere of jurisdiction (Awotayo*et al*., 2013). The incursion of the military into governance, and the consequent imposition of military command structure in a federation set the tone for the distortion of Nigeria's federalism. Thus, the practice of federalism in Nigeria no doubt has been distorted by overwhelming dominance of the federal government that distributes national resources to lower level government at its own whims and caprices (Ewetan, 2011).

Since independence, the demand for true federalism, fiscal and political restructuring by different ethnic nationalities in Nigeria

DOI: https://doi.org/10.63725/jpsp.v14i1.01

has not abated. These agitations have contributed to violent rebellious reactions by aggrieved ethnic groups in the country, endangering the security, unity, and corporate existence of Nigeria as one country. Federalism that undermines the independence and autonomy of its federating units will only bring about conflict, threat to national cohesion and peace, and ultimate disintegration (Ali, 2013; Adamu, 2005).

Insecurity challenges can be traced to the early years of military rule when large quantities of arms were imported into the country for the use of the military during and after the Nigerian civil war, some of which got into the hand of the civilians. Soon after the civil war these arms were used by civilians and ex-military men for mischievous purposes such as armed robbery. There was also the army of unemployed youths some of whom lost their job during the civil war. The level of insecurity assumed dangerous dimensions in the prolonged years of military rule beginning from 1970 during which people procure arms and light weapons for personal defence; some of these arms and light weapons got into the hands of unemployed youths who used them for deviant purpose. While some researchers attribute youth violence to peer group influence and other psychological factors associated with growing up, others emphasised the impact of political and economic factors such as ethnic agitation, political agitation, unemployment, Structural Adjustment Programme (SAP) as triggers of violent reaction among the youth. Many scholars have identified several causes of conflict and insecurity in Nigeria that are inimical to socio-economic and national development (Jega, 2002; Okorie, 2011; Ali, 2013). These causes have been classified into external and internal causes. In Nigeria the internal causes of insecurity pose major challenge to socio-economic development than the external causes of insecurity.

Theoretical Framework

Risk management theory of information security The Risk Management Theory was developed in 1970s by the psychologists Amos Tversky, Daniel Kahneman, and Paul Slovic. This idea came into existence when they investigate the ways by which people make decisions under uncertainty or risk. "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resources to the organisation" (Vines, 2003). There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasure (computer) (controls) used to manage security information must strike a balance between the given data, the security personnel who controls the information and the value of the informational asset being protected.

Apparently, risk in this sense is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to inflict harm, it has an

DOI: https://doi.org/10.63725/jpsp.v14i1.01

impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk.

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use some qualitative analysis based on informed opinion, or where reliable dollar figure and historical information is available, the analysis may use quantitative analysis. When management chooses to mitigate a risk, they will do so by complimenting one or more of three different types of controls.

An important aspect of information security and risk management is recognising the value of information and defining appropriate procedure and protection requirements for the information. Not all information is equal and so not information requires the same degree of protection. This requires information to be assigned a security classification.

Methodology

Descriptive research design was adopted for this study through the use of quantitative method. The purpose of using descriptive research is to determine the situation, as it existed at the period of study and to interpret out the findings in the questionnaires. It also aided in simplifying the work through drawing of inferences about the target population from investigation of the few. A questionnaire was designed based on the objectives of this study; it was distributed and retrieved in order to get the accurate outcome after the exercise.

The population of this study comprises all the senior personnel of Ibadan North Local Government Area Oyo state, which include male and female. Simple random sampling technique was adopted in selecting the sample for the study. The sample represents the entire numbers of the personnel. 80 copies of questionnaires were randomly administered for the process of gathering data from the study area. The technique that was adopted is the statistical descriptive method; the overall responses were ascertained and recorded with statistical tools like response, frequency, percentage, and total. The presentation was done in simple tables and percentages, under which analysis of each question was done. Both primary and secondary data gathered were then used in answering the research questions of this study.

Conclusion

Information security management should be seen as strategy rather than merely operational routine. The gathering of information must not be taken for security protection itself. It must be processed, analysed and managed for sound intelligence sharing and decision making. The security of information can be said to be managed if it protect the confidentiality of the data, preserve the integrity of the data and promote the availability of the data for authorised use. A threat to the information security in a community could jeopardise the stability and peace of the society and if not swiftly addressed, can trigger violence and lead to peace disruption in a society. Information security management is vital among security agencies as it enhances peace in the community and holistic prevention of crime and insecurity.

DOI: https://doi.org/10.63725/jpsp.v14i1.01

Information gathering and prompt process of the same can avert conflict in the society. It is evident from the study that information security management remains a vital key in peacebuilding, detecting, preventing and responding to threats and vulnerable attacks in any society. The flow of communication within the community facilitates intelligence gathering, information sharing, security mappings and surveillances for prompt response to possible insurgence.

However, the challenge of upgrading or procurement of relevant equipment and tools needed to ensure swift flow of information for timely response is slowed down due to poor funding. Moreover, ISM provides avenue through which root causes of conflict that produces threat in the society are discovered; this however as proven also to enhance peacebuilding and conflict management within a violent prone society.

Recommendations

1. A sound state/community nexus of conflict management and peacebuilding should be strengthened for both local and community engagement because it should be seen as strategic rather than merely operational.

2. Overhauling of information security management apparatus for timely, effective and efficient communication is necessary at Ibadan local government area as outdated tools and equipment can compromise information security.

3. Actionable intelligence with simplified information-sharing within departments and agencies should be prioritised as this would foster synergy between civilian and internal security.

4. Ibadan North LGA should partner civil society organisation and other actors in educating the populace on knowledge sharing initiatives on information security management awareness.

REFERENCES

Achumba, I. C., Aghomereho, O. S. and Akpor-Robaro, M. O. M. 2013. Security challenges in Nigeria and the implications for business activities and sustainable development. *Journal of Economics and Sustainable Development* 4.2: 79-86.

Adagba, O., Ugwu, S. C. and Eme, O. I. 2012. Activities of Boko Haram and insecurity problems in Nigeria. *Arabian Journal of Business and Management Review* 1.9: 13-27.

Adamu, A. 2005. *True federalism in the 21st century Nigeria*. A Lecture Delivered at University of Jos Alumni Association, Lagos, 24th March.

Adeola, G. L. and Oluyemi, F. 2012. The political and security implications of cross border migration between Nigeria and her francophone neighbours. *International Journal of Social Science Tomorrow* 1.3: 1-9.

Al-Rodhan, N. R. F. 2007. *The five dimension of global security: proposal for a multi sum security principle*. Berlin: LIT Verlag.

Anderson, J. M. 2003. Why we need a new definition of information security. *Computers & Security* 22.4: 3-8.

Appadorai, A. 2004. *The substace of politics*. New Delhi: Oxford University Press.

Bajpai, K. 2000. Human security: concept and measurement. University of Notre

DOI: https://doi.org/10.63725/jpsp.v14i1.01

Dame, Kroc Institute. *Occasional Paper* No. 19.

Balwin, D. 1997. The concept of security. *Review of International Studies* 23.1: 101-113.

Basie, V. S. 2005. Information security governance – compliance management versus operational management. *Computers and Security* 24.6: 443-447.

Beland, D. 2005. The political construction of collective insecurity: from moral panic to blame avoidance and organised irresponsibility. *Centre for European Studies, Working Paper Series* 126.

Clover, J. 2003. Food security in sub-Saharan African. *African Security Review*, 12.1.

Cortada, J. W. 2010. *How societies embrace information technology: lessons for management and the rest of us*. Hoboken, NJ, USA: John Wiley & Sons, Inc.

Danbazau, A. B. 2007. *Criminology justice* (2nd edition). Ibadan: Spectrum Books Limited.

Daniel, I. A. 2011. Intelligence information and policing in Nigeria: issues and way forward. *The Journal of International Social Research* 4.17: 474-484.

Davies, A. E. 2009. *Food for security initiative in Nigeria: prospects and challenges*. Monograph, Department of Political Science, University of Ilorin.

Edeko, S. E. 2011. The proliferation of small arms and light weapons in Africa: a case study of the Niger Delta in Nigeria. *Sacha Journal of Environmental Studies* 1.2: 55-80.

Egbewole, W. O. 2013. *Security challenges: the role of the Nigerian woman*. Keynote Address presented to the Annual Conference of the International Federation of Women Lawyers (FIDA) Kwara State Branch on 19th March, 2013.

Egwu, S. G. 2001. *Ethnic and religious violence in Nigeria*. Jos: St. Stephen Book House.

Eide, A. 1999. Globalisation, universalisation and human rights to adequate food. *'Not By Bread Alone' Food Security and Governance in Africa*. Eds. A. Ogunrinade, R. Oniango& J. May. New York: A Publication of Toda Institute for Global Peace and Security. 78-91.

Eloff, M. and Solms, V. 2000. *Information security: process evaluation and product evaluation ENISA (European Network and Information Security Agency)*. Risk Management /Risk Assessment (available on-line at http://www.enisa.europa.eu/rmra)

Ernst and Young, 2012. *Fighting to close the gap*. Retrieved from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Securiy_Survey/$FILE/2012_Global_Information_Security_Survey_Fighting_to_close_the_gap.pdf.

Ewetan, O. O. 2011. Fiscal federalism and macroeconomic performance in Nigeria. Ph.D. Thesis, Covenant University, Department of Economics and Development Studies.

Ezingeard, J. and Bowen-Schrire, M. 2007. Triggers of change in information security management practices. *Journal of General Management* 32.4: 53-72.

Farrell, R. 2012. *Boko Haram: understanding the threat*. New York: Consultancy Africa Intelligence's Conflict and terrorism Units.

DOI: https://doi.org/10.63725/jpsp.v14i1.01

Grant, K., Edgar, D., Sukumar, A. and Meyer, M. 2014. Risky business: perceptions of ebusiness risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management* 34.2: 99-122.

Grizold, A. 1994. The concept of national security in the contemporary world. *International Journal on World Peace* 11.3: 41-56.

Hazen, J. M. and Horner, J. 2007. *Small arms, armed violence, and insecurity in Nigeria: the Niger Delta in perspective*. Switzerland Small Arms Survey.

Ibrahim, J. and Igbuzor, O. 2002. *Memorandum submitted to the presidential committee on national security in Nigeria*.

ILO, n.d. *Definitions: what we mean when we say 'economic security'*. Retrieved September 5, 2016.

ISO/IEC 27002, 2005. *Information technology: security techniques (code of practice for information security management)*.

Iyare, T. 2008. Corruption and the crisis of national values. *Governance and Politics in Nigeria: The IBB and OBJ Years*. Ed. J Oyovbaire. Ibadan: Spectrum Books Limited. 20-31.

Jega, I. 2002. Tackling ethno-religious conflicts in Nigeria. *Newsletter of Social Science Academy of Nigeria*, September 5.2: 35-38.

Jekins, J. C. and Scanlan, S. J. 2001. Food security in less developed countries 1970-1990. *American Sociological Review* 66.

Li, *et al*. 2003. *BS7799: a suitable model for information security management*.

Nwagboso, C. I. 2012. Security challenges and economy of the Nigerian state (2007 – 2011). *American International Journal of Contemporary Research* 2.6: 244-258.

Nwanegbo, C. J. and Odigbo, J. 2013. *International Journal of Humanities and Social Science* 3.4: 285-291.

Ogah, D. 2011. *Expatriates, some semi-skilled, take over even menial jobs from Nigerians*. Retrieved February 2, 2012, from http://www.guardiannewsngr.com/index.php ?

Okorie, I. 2011. *Insecurity: consequences for investment and employment*.

Olonisakin, F. 2008. In the line of fire. *BBC Focus on Africa* (April-June), 19-23.

Oluwarotimi, A. 2012. US to use more balanced security strategy to fight insecurity in Nigeria. *Leadership* Newspaper, 2 June.

Onifade, C. A., Imhonopi, D. and Urim, 2013. *Towards national integration in Nigeria: jumping the hurdles*. A paper presented at the 28th National Conference of the Social Studies Association of Nigeria, Themed: "The Unending Question of National Unity in Nigeria – In whose Interest?" Institute of Education, OAU, Osun, November 26 - 29, 2012.

Onouha, F. C. 2011. Nigeria's vulnerability to terrorism: the imperative of a counter religious extremism and terrorism (CONREST) strategy. *Peace and Conflict Monitor* (2 February). Retrieved from: http://www.monitor.upeace.org/ inner pg. cfm?id

Oshio, E. 2009. *The challenges of national security and development*. Being a paper delivered at the Delta State Christian Professional League Seminar on Crisis Management and Nation Building. Grand Hotel, Asaba, Thursday, 19th November.

DOI: https://doi.org/10.63725/jpsp.v14i1.01

Poneman Institute, 2012. *2011 cost of data breach study: United States*. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Pulkkinen, M., Naumenko, A. and Luostarinen, K. 2007. Managing information security in a business network of machinery maintenance services business – enterprise architecture as a coordination tool. *Journal of Systems and Software* 80.10: 16071620.

Salawu, B. 2010. Ethno-religious conflicts in Nigeria: casual analysis and proposal for new management strategies. *European Journal of Social Sciences* 13.3: 33-45.

Werlinger, R., Hawkey, K. and Beznosov, K. 2009. An integrated view of human, organisational and technological challenges of IT security management. *Information Management and Computer Security* 17.1: 4-19.

Whitman, M. E. 2004. In defense of the realm: understanding the threats to information security. *International Journal of Information Management* 24.1: 43-57.

DOI: https://doi.org/10.63725/jpsp.v14i1.01