Achieving information safety in a disaster environment: the way forward for Africa

Janes Ouma Odongo
Department of Governance and Public Policy
The Technical University of Kenya
Nairobi, Kenya

Email: odongojanes@yahoo.com

Abstract

Rationale of Study – Disaster incidents are becoming common globally. When they occur, disasters are known to cause great havoc resulting in high numbers of human fatalities and injuries; massive damage and destruction of property; and high degrees of strain on environmental resources. In most cases, people only associate Africa's disasters with humanitarian consequences while completely ignoring other forms of damages and losses caused therein. The impact of disasters on records and information in Africa is generally ignored.

Methodology – Based on a desk review of secondary data, this descriptive study explored the information capabilities, potentials and risks that Africa has which can be threatened by disasters.

Findings – The findings of the study indicate that although records management in Africa is still largely paper-based, electronic records management is picking pace across the continent in line with current global practice. However, the limited use of digital document signing technologies means that official signed records still have to be kept in hard-copies. This poses threats to records during emergencies.

Implications – The author recommends that a more holistic approach should be taken in discourses regarding Africa's disasters and their management. Most importantly, there should be meaningful disaster management focused on ensuring information security before, during and after disasters. This is considering that even disaster recovery efforts are largely hinged on the safety of these records.

Originality – Although it used secondary data, this study was original in terms of its scope and coverage. It emphasises that emerging technologies that enable records to be processed, signed and stored without printing should be used to ensure environmental and information safety during disasters.

Keywords

Information security, disaster management, development, Africa

Citation: Odongo, J.O. (2018 Achieving information safety in a disaster environment: the way forward for Africa. *Regional Journal of Information and Knowledge Management*, 3 (1),15-29.

Published by the Regional Institute of Information and Knowledge Management
P.O. Box 24358 – 00100 – Nairobi, Kenya

1 Introduction

A review of global statistics indicates that Africa is among the safest continents in as far as tumultuous disaster incidents are concerned. For a very long time, the continent has not been hit by disasters such as massive earthquakes, volcanic eruptions, hurricanes, cyclones and infernos (UNISDR, 2016). The most recent such activity was the mudslide in Sierra Leon in 2017 for which comprehensive statistics on information losses do not exist. However, this does not imply that the continent does not experience disasters of its own. Actually, the continent has among the highest number of recorded fatalities and victims affected by disaster incidents during the 20th and 21st centuries. These losses are majorly attributable to conflicts, droughts, disease outbreaks and floods that occur from time to time in different countries in the continent. The high number of human losses associated with disasters in Africa, as witnessed over the last one decade (1996-2015), is majorly due to inadequate disaster preparedness and response. This is consistent with global data on disaster trends from low income and low-middle income countries over this period (Guha-Sapir *et al.,* 2016).

By their very nature, Africa's disaster incidents, as common as they are, may not pose the greatest threat to information security. This, according to those who hold this belief, is most likely the case because the continent rarely experiences disaster incidences that are associated with earthquakes, mass movement of earth matter, or fast-moving winds and precipitation as is common along the eastern coasts of the Pacific and the Atlantic oceans (Guha-Sapir *et al.,* 2016). In the areas where they occur, for example along the coasts of Japan, China and the United States of America, these incidents are known to sweep away buildings and other manmade structures that fall on their course and in the process dump records to conditions beyond salvage. But is it true that records are safer in Africa than elsewhere in the world just because the continent is exposed to a different type of hazards?

In most cases, the natural course is that during disasters, developed countries experience more financial and information losses as opposed to human deaths and injuries due to high levels of preparedness to counter such calamities. In least developing countries, however, disasters result in more human as opposed to material losses. This is mainly due to lack of preparedness for disasters which expose people to the full force of natural and man-made catastrophes. Here, the engineering works meant to hedge populations from danger are mostly lacking or underdeveloped largely due to underinvestment. Further, the high human, as opposed to material losses, are due to the fact that unlike in developed nations, developing ones experience lower levels of economic investment in actual fiscal terms. That is not to say that material losses do not exist during disasters in less developed countries where most African countries fall (UNCDP, 2017; UNCTAD 2016). It also does not imply that there are no information security risks during disasters in these countries (MSNHCK, 2009). As a matter of fact, all people, whether in rich or poor countries, attach the same significance to their property (including documents and other records) that can be lost or damaged during disasters. It, therefore, means that information security and safety should be a consideration for all countries, including those in Africa.

2 Statement of the research problem

Although it may seem that Africa only experiences droughts, floods and epidemics which do not remarkably threaten records, specific institutions experience fire outbreaks from time to time, or such other calamities that result in them losing their information records. In Nairobi, for instance, the county government's fire department reports that its staff respond to 760-800 fire emergencies annually (Mbugua, 2015; Wachira and Smith, 2013). Most of these fire outbreaks occur in office blocks, factories in industrial districts, slum dwellings and at people's homes (Ford, 2013). The risk of information loss existent in these incidences cannot be ignored.

In a more globalising world, today, various African cities are headquarters to different multinational institutions with mega information needs as well as investments on and high stakes in records keeping and management (Luiz and Radebe, 2012). Therefore, in as much as one would like to paint the image of Africa as a poor continent where the only needs with regard to disasters are humanitarian, the contrary is true. Africa is home to many records relating to transactions of millions of governmental and non-governmental institutions that operate within the continent. Similarly, the record keeping and management needs of the individuals and families that live within the cities and villages of Africa should be considered. Do they have any information security fears? Have they ever experienced information loss? What are the likely impacts of disaster-induced information losses to the various stakeholders identified above? These are concerns that need to be established and documented.

While answering the above important questions, consideration should be given to the fact that Africa is home to some of the fastest growing economies of the world today (UNCTAD 2016; African Development Bank, 2017). The continent's risks and needs are expected to change with its changing fortunes. Moving forward, people should expect Africa's disaster management stakeholders' focus to shift from humanitarian emergency response centred on providing food, shelter, clothing and medical care to disaster victims, to giving more attention to guaranteeing business continuity in post disaster scenarios for individuals and institutions alike. Achieving this requires resilient records systems.

As a pointer to this need, it should be noted that several incidences are often reported across the globe where communities and organisations are not even able to account for individuals, assets, losses and liabilities because all their documents have been lost during disaster outbreaks. There have also been reports of family members losing all their identification, academic papers, property ownership and insurance documents when their homes are damaged or destroyed in disasters. Such families and organisations are forced by their circumstances to begin their lives again from scratch or start assembling these documents from third parties who keep copies. This can be a very expensive undertaking.

3 Methodology

This study employed a descriptive research design. Its findings are a product of a desk study involving content analysis of relevant literature including books, journal articles, policy documents and Internet content conducted by the researcher. The researcher used scientific inference to descriptively draw a meaning from the literature and then make recommendations and conclusions on the issues under investigation. The findings are derived from the data collected and analysed from documentary evidence accessed by the researcher.

4 Findings

Ordinary information management practices in a non-disaster environment

The study established an acknowledgement that proper records management is necessary for effective governance of any affairs, whether of an individual, family, business, any other institution or even the state (Ngoepe, 2008). People and organisations believe in keeping vital records for future reference, or as documentation of transactions. This is typically necessary to confirm ownership of assets or qualifications of some sort. There is no guarantee that all these documents actually find use in the course of their existence (Posey 2010).

In most cases, and with a majority of people, record keeping is done as a formality. Documents and files are created for no apparent reason and are kept unused in cabinets and stands where they gather dust for years without anybody making reference to them. That this happens still does not mean that the records are not important (Posey 2010). Such files are majorly kept for audit purposes and most audits happen once in a year if not once in every five to ten years. It is hence not surprising to find that a document kept in a filing cabinet somewhere within an organisation will be read just once or twice in a span of twenty years. Such a document will nonetheless still need to be kept around since lack of it can be a condition for other chaos in the organisation in future (Halsted *et al.,* 2005).

The greatest risk posed by infrequent interactions with documents is that in most cases, they are not updated, cleaned, repaired, or checked for security and safety. In effect, even under ordinary non-disaster circumstances, accessing documents becomes difficult. This is particularly so on occasions when, due to poor handling added to the element of tear and wear, even indexes or serial numbers disappear making it difficult to know which document is where. It is also expected that such documents get torn with time making the information they contain inaccessible. Incidences also exist when documents get mixed up and lost in piles. Under such conditions, it can take days, if not months, to go through records and recover a misplaced file.

Many organisations report that proper record keeping has declined to the point that it is becoming a hazard, especially in government institutions (Ngoepe, 2008) where files are only kept as active records for three months or less before being archived or destroyed. This increase in poor record keeping is majorly attributed to over-reliance on computers to keep information for future reference. There also exists the reluctance to print documents in many organisations in which printing is associated with both great costs of buying paper and printers, as well as environmental degradation with environmentalists warning that just like charcoal burning and harvesting of wood fuel, paper production is contributing greatly to the reduction of the global forest cover (BCIT 2011). People would therefore rather keep soft copies of files than print and contribute to the global warming menace. All the same, this apathy contributes to poor filing in offices.

Though one would want to praise the introduction of computer technologies for reducing the burdens associated with record keeping for organisations, the use of computers and servers to store documents poses another risk. Documents kept in computers are sometimes lost when computer hard drives crash. In addition, the security and safety of such information may be difficult to guarantee as it can even be accessed remotely by ill willing parties. One also needs to note that documents kept in computers are vulnerable to viruses and other computer bugs that can completely delete an organisation’s records and leave it with nothing to refer to (United States Department of

Education, Privacy Technical Assistance Centre, 2011). Hence, the best approach is to use both soft copy and hard copy records to complement each other. Whereas hard copies are vulnerable to tear and wear, as well as being burnt by fires, soft copy files are relatively resistant to this threat. On the other hand, hard copy files cannot be affected by computer viruses. Organisations are reporting a declining role of physical filling techniques due to man-power and space considerations. The documents are also a hazard and can potentially fuel fires or be soaked and lost in floods. The use of electronic records is gaining currency globally and is a more ecologically friendly alternative in this era of global warming.

Even under normal circumstances, organisations struggle with making the decision on which documents to destroy and after they have been stored for how long (Rockefeller Archive Center, 2008). It is not easy to know when an archived document may be needed next. Therefore, most people would rather have these documents in the store somewhere than destroy them completely. But this poses the danger of these landing in the wrong hands, especially in emergency situations. It is noted too, that the longer a document stays in storage, the more careless people become with handling it. Since they are dusty, the records may end up thrown carelessly in heaps in a room somewhere. But that does not mean that some ill-intentioned individuals cannot rummage through the debris, find the documents they want, and use them against the organisation, for example, in a law suit.

The other danger is that in most occasions, after keeping documents for many years without using them, people in organisations consider them as garbage which is usually just carried away to the dumpsites with other wastes without being shredded or burnt. When such documents get into the wrong hands, they can be used to unearth long buried events. These can be a source of great embarrassment and financial burdens in legal duels and reparations to victims of those events. They lead to the closure of organisations due to loss of reputation, finances and a multitude of other accompanying ramifications.

In general, records management is equally challenging for both individuals and organisations even under ordinary business environments. It poses a space, human resource and financial constraint that they would rather do without. Still, organisations need records and must keep them. Consequently, they have the challenge of choosing between electronic and hard copy methods of record keeping, of training their employees on the best practices in record keeping and information management, and of ensuring that when done with, past records are disposed in a safe way so that they cannot be used by ill-intentioned parties to wake up “old ghosts” that would haunt affected institutions and parties. In the face of these concerns, there is a need to pay special attention to information management concerns that exist during disaster situations.

Modern day information security related emergencies

Currently, one of the major causes of information losses in Africa is fire outbreaks. Fire emergencies are very common both at the household and organisational levels across the world. Another major challenge is computer-based attacks on information. These can be in the form of hackers, viruses, bugs or any other type of computer-based threats to data safety (Millar, 2009). Computer-based information security threats are becoming even a bigger concern. This is because of the growing ubiquity of computers globally. In 1977 there were fewer than 50,000 personal computers in use but as of January, 2017, over 3.7 billion people globally had access to electronic devices with the capacity to process and store information (Millar, 2009). These included computers and phones. A similar number of people had access to and used the Internet hence exposing them to online data threats (Kemp 2017). This points to the fact that information production, consumption and management has shifted from paper-based access to computer-based options. Consequently, this is where the threat is also shifting to. Perhaps the most recent indicator of this problem is the complaint by the American Democratic Party that Russia helped to rig the country’s 2016 presidential election in favour of Mr. Donald Trump. Another similar complaint is that of the Kenyan opposition party claiming that the presidential election results in the country’s 2017 elections were generated or manipulated remotely using computers.

Still, even with the advent of the modern technologies, traditional information records are at risk of being consumed by fire across Africa. This is majorly because fire emergencies, especially those affecting offices and homes, are on the rise across the continent due to increasing human population, high demand for office and residential space, and the ensuing congestion in available spaces. These conditions increase the likelihood of fire outbreaks and their rapid spread. In congested office spaces, for instance, large stacks of paper, even if they be records, can act as fuel and make fires even more ferocious (IFRC, 2009; Ford, 2013). Another risk factor that contributes to faster spread of fires is the increasing cost of construction and the subsequent introduction of cheaper building partitioning technologies. These partitions are done using wood and boards that easily facilitate the spread of fire. This is unlike the case in situations where buildings are partitioned using stones (Litch and Brink, 2015). To guard against this risk factor which is engrained in building designs themselves, questions will have to be asked on whether cheap building and partitioning designs are expensive in the longer run or not. Consideration will also have to be made of the facts of how to cure the deficiencies in the designs already used with the goal of avoiding fire outbreaks instead of altering the buildings themselves which may be even more costly.

Information security threats infused in all types of disasters

Other than what is discussed in the above section, the study established three major information security threats that one must consider when dealing with any type of disaster. Some of these threats are inbuilt within the disaster incidents themselves but others are secondary outcomes, usually due to third parties taking advantage of the eventualities to “nose around”. This is not to say that a number of the events happen by chance. The three major threats are: 1) the risk of information being consumed in a disaster – whether burnt, soaked, or buried; 2) the risk of information being accessed by unauthorised persons; and 3) misplacement of information hurriedly moved to the wrong location.

Information loss in disasters

In an emergency of any kind, physical or tangible materials will experience damage or complete destruction. These materials can be a car, building, or even a filing cabinet. In the case of documents, most of them are typically lost through either being too soiled to the extent that recovering them is impossible; being drenched in water (or any other liquid) and lost therein; or being razed into dust by fires. Whichever the case, when this happens, the affected information will be completely lost, and, unless the concerned institution had backed up their data elsewhere, they will completely lose these hard copy documents. They can also, due to lack of records, disseminate the wrong information to the publics (NDMA, 2013; Halsted *et al.,* 2005). Disaster events can completely erase the information memory of an institution and open it up to associated risks from clients and competitors who can come up with all sorts of claims against it.

Similarly, organisations can still lose electronic records in disasters through the damage of servers in which information is kept. In some occasions, the hard drives containing information can be burnt, broken into pieces, or soaked by other substances making them not to work again. Unlike the case with paper documents, some hope exists with electronic records in the sense that information technology experts can be engaged to reconstruct the damaged memory and retrieve the lost information. This is not possible in all occasions, but it can be done (Garner, 2010; FBI, 1984), and is among the key reasons why electronic record keeping is gaining prominence.

The final way through which information loss occurs during disasters is theft. Here, whoever steals the information may not necessarily intend to use it in any way but can just pick up the documents or disks out of curiosity. Whether such information is used elsewhere or not, theft here basically refers to one taking these records without prior permission. The documents can as well end up being shredded and used to make *papier mache*.

The risk of information being accessed by unauthorised persons

The study established this to be the second form of information safety risk associated with post disaster environments. Occasionally, there are instances when, as a result of the confusion that follows an emergency, custodians of vital information may lose their grip on it. Such confidential data can end up in the wrong hands, and can be used to reveal secrets, tarnish the name of the organisation, and so forth. As said earlier, when information is accessed in such a manner, it can expose the secrets that an organisation had long buried. These are capable of resurrecting issues between affected companies and other stakeholders and can be a cause of long-winded and costly legal battles.

The most closely related scenario to this challenge is Julian Assange's Wikileaks saga. From 2016, Wikileaks has had unauthorised access to over ten million confidential documents owned by various government institutions and private corporations around the world. These vital documents were then shared by the organisation through the World Wide Web. The secrets exposed by these documents have caused a firestorm in quite a number of affected institutions resulting in executive-level resignations, collapse of institutions and arrests of individuals implicated in the leaks, among other consequences (WikiLeaks, 2016). One does not need to look so far away to know the impact of such document leaks. In Kenya, for instance, a few individuals, including powerful government ministers, were revealed to have misappropriated state funds through a Wikileaks dossier in 2010. This revelation saw those implicated resign and investigated by the governments of Kenya and the United Kingdom. Unfortunately, however, the investigations have not been concluded several years down the line.

Sometimes, information can be stolen even during disaster response. This can be so when responders deliberately pick files in the process of doing their work. It is an unethical practice that should be penalised severely but such misconduct can occur and cost organisations greatly especially when the parties in question do not adhere to operational oaths of secrecy which bar them from providing operational details without prior permission.

With regard to electronic records, as may have been mentioned, disaster situations are marred with confusion. In such situations, system administrators may lose their control of servers and computer databases to unscrupulous online thieves (Yu, 2015; Robinson *et al.,* 2011). A disaster environment can expose online documents to hackers and espionages considering that during emergencies, some systems may even stall leaving organisational servers exposed to remote manipulation. It would not be strange for someone to transfer all files to another location or introduce bugs into the systems to corrupt the files stored therein. Organisations whose operations can be severely affected by such losses include banks, national security agencies, academic institutions, and any other organisation that handles sensitive or highly confidential computer-based (including online) documents. It is also worth noting that some of these espionages purely trade in such information. Any vital records they steal usually find themselves in the market being sold to willing buyers who will use them against their original owner (Yu, 2015).

Misplacement of information

Organisations can temporarily lose information during a disaster through misplacement. This occurs when during emergency response, materials are moved out of harm's way very fast and carelessly without following any specific order. In this case, documents may end up being mixed up with other items. Thus, the initially employed filling systems and order is interfered with making documents into a fumble (or just any heap of papers). Even after the disaster has been managed, it may take a lot of effort to put such documents back in order. There is also a high probability that at least a few of the documents will never be recovered when needed either because they were finally stolen or damaged, or that they just got completely buried in the wrong heap and were not found. Though misplacement of files during emergencies does not pose an immediate information security threat, it can still happen when such documents either end up in the wrong hands or get lost.

5 Conclusion and recommendations on how to tackle information security risks in disasters

Based on the established trends, it would be misleading to say that Africa has not invested enough in information management and security (SERIANU, 2016; Symantec, 2016). Efforts have been put in place to secure documents through the use of warehouses, shelves and filing cabinets. Organisations, including libraries, have through time used modern technologies to keep records safe (Government of Kenya, 2009; Katuu and Ngoepe, 2015). However, this is not to say that more should not be done. In fact, the continent needs to put in more effort in embracing modern technologies that are used globally to secure records from the current disaster threats. Compared to other parts of the world, Africa is still playing catch up with the current data security practices used in the technologically advanced parts of the world.

Although most focus is usually given to current (active) records, organisations should also strive to secure semi-active and non-active records both during normal times and during emergencies. This is also recommended by Kenya's Public Procurement Oversight Authority [PPOA] (2010). Old archived documents are known to raise serious issues when accessed by wrong parties, especially following disasters. In most cases, it is recommended that organisations shred and dispose old and unneeded documents after certain periods. Before this is done, such documents should always be kept secure under lock and key and with access to only authorised persons. Old records in hard disks, including damaged disks used for keeping electronic records, should also be deleted and destroyed in a manner that they makes them not to be recovered and used by ill meaning parties.

To achieve the greatest standards of information safety and security, organisations should invest in recruiting and regularly training records managers. These individuals can be tasked with updating records and also formulating and implementing policies on records safety. In addition, records managers, through regular research, can upgrade organisational record keeping technologies in line with the emerging trends in the market. In so doing, they ensure that their establishment is aware of the most current information risks, and that it invests in technologies needed to keep it secured from such risks.

There is need for organisations to invest in bugler proof, fire proof and water proof storage that can hold vital documents during emergencies. As noted earlier, the greatest threats to information security at all times but mostly during disasters are thieves, water and other liquids. It is best that they are kept away from accessing records through investment in technologies that can guard against the same. This measure is important for securing both hard copy and electronic records.

On another note, there should be limited (or controlled) access to disaster sites immediately and even long after the incident by spectators.

Some of the "supposed to be spectators" during disasters have been known to loot property and even carry away vital records. It is therefore recommended that such sites be completely cordoned off from the public glare; access given specifically to authorised persons; and records be kept of those who walk into and out of such sites from the time the disaster strikes to the end of the operation when such property is handed back to the managers. It is also imperative that an individual or a unit be set up to receive, record, and keep custody of any documents and disks recovered from the site. Such should also be immediately brought to the attention of the organisation's official record keepers.

In recent the years, organisations have taken up the idea of investing in offsite data centres. These are establishments in their own accord with staff and other resources employed around the clock to organise, store, clean, maintain, retrieve, and secure records from harm's way. It is recommended that organisations should not just be satisfied with having one data centre, but depending on the nature of its information needs, one can decide to have as many centres as possible, scattered across geographical locations so that at least, data in one site will be safe at any given time if disasters were to strike.

As a rule of the thumb, data centres should be located at the most secure places possible. Data centres should always be free from electricity outages, floodplains, earthquake and storm prone areas, and should have a 24/7 security system. Usually, organisations prefer to have these centres hidden under mountains, near military barracks, or in a diplomatic community (set up) where security breaches are highly unlikely. They should also be installed with layers of online data security systems which make them impregnable by viruses, worms, hackers and espionages. Such centres are coming up in major cities across Africa including in Nairobi, Lilongwe, Cape Town, Abuja and Addis Ababa (Global News Wire, 2017; Source8, 2015; Xalam Analytics, 2015), and are particularly necessary for keeping records from sensitive government departments, banks, other multinational corporations and such agencies.

Usually, due to the high costs associated with setting up data centres, it can be recommended that organisations can acquire their storage space through a rent-a-space programme with other agencies that have more storage capacities than they need. There also exist institutions that set up and manage such centres purely for rental purposes. Therefore, an institution can have its primary data centre in-house, but still rent back-up storage space in other agencies elsewhere, even in other cities, so as to cushion itself from the risks of data loss but at a cheaper price. The traditional equivalent of this is the renting of safe deposit boxes in banks. This has been a global practice for decades. The emergence of data centres is a more secure and cheaper alternative. This is even more so because today, even hard copy documents can be scanned and stored in these electronic stores so as to save on space needs. Such facilities can hold large amounts of data in a very small space. Data centres installed with voluminous servers are cheap to operate and secure. They are also environment-friendly in the sense that this way of storing information can save acres of forest land in tree that would have been cut to produce paper for printing hard copies. With their rent-a-space model of use, one data centre can serve many organisations.

The traditional over-dependence on paper records should be done away with. Managing paper records is both unsafe and expensive. Global statistics show that most office fires are started by electrical faults but fuelled by paper in such environments. Expectedly, the bigger the amount of paper in an establishment, the higher the chances of losses being incurred if a fire emergency was to occur. In addition, paper records are threatened by not only fire but also liquids, including water. During storms and floods, paper records can easily be soaked by water and completely destroyed. This is unlike electronic records in disks which are relatively easier to secure. As explained earlier, paper use is also a threat to the environment through its dependence on trees whose felling contributes to deforestation and the global warming effect. The solution to over-dependence on paper records also requires the invention and investment in affordable technologies that can make it easy and cheaply possible to work on and sign a document in its electronic format without having to print it. Surprising as it may sound, most people and organisations print documents just so that they can be signed and stored. This happens not because the electronic version of these documents is of less use, but because they cannot be signed in electronic format. Additional help to facilitate electronic record keeping can be through making scanners more affordable to members of the public and tightening security for electronic records by keeping off hackers and viruses.

6 References

African Development Bank Group, (2017) African Economic Outlook 2017; Entrepreneurship and Industrialization, Abidjan, Nigeria, African Development Bank Group.

Brink, V.V.D. (2013) *Fire Safety and Suppression in Modern Residential Buildings*, Eindhoven, Netherlands, Eindhoven University of Technology.

British Columbia Institute of Technology (2011) *Records Management Procedure,* Records Management and Privacy, British Columbia, Canada, British Columbia Institute of Technology.

Federal Bureau of Investigation [FBI] (1984) *Law Enforcement Records Management Systems (RMSS),* Washington DC, United States of America, U.S Department of Justice.

Ford, S. (2013) *South Africa's Three Billion Fire Loss Statistic,* Lexis-Nexis Property Law Digest, March 2013, P8- P10, South Africa.

Garner, F. (2010) *Records Management Systems: Backup Systems, available on:*

Global News Wire (2017) *African Data Center Markets 2017 - How the Race to the Cloud is Transforming African Colocation Markets*. Available on:

Government of Kenya, Ministry of State for National Heritage and Culture, MSNHCK, (2009) *Draft National Policy on Records Management,* Nairobi, Kenya, Ministry of State for National Heritage and Culture.

Guha-Sapir, D., Hoyois, P. and Below, R. (2016) *Annual Disaster Statistical Review 2015: The Numbers and Trends*. Brussels, Belgium, CRED; 2016

Halsted, D.D., Jasper, R.P. and Little, F.M. (2005) *Disaster Planning; A How-To-Do-It Manual for Librarians,* New York, USA, Neal-Schuman Publishers Inc. *http://www.iacptechnology.org/ttap/RecordsManagementSystems.pdf.* http://www.source8.com/wp-content/uploads/2015/01/African-Data-Centres-FINAL.pdf https://globenewswire.com/news-release/2017/07/21/1055702/0/en/African-Data-Center-Markets-2017-How-the-Race-to-the-Cloud-is-Transforming-African-Colocation-Markets.html

International Federation of the Red Cross and the Red Crescent [IFRC] (2014) *World Disasters Report 2014; Focus on Culture and Risk,* Geneva, Switzerland, *International* Federation of Red Cross and Red Crescent Societies, 2014, ISBN 978-92-9139-214-8.

International Federation of the Red Cross and the Red Crescent [IFRC] (2009) *Kenya: Fires,* Nairobi, Kenya, International Federation of the Red Cross and the Red Crescent.

Katuu, S. and Ngoepe, M. (2015) *Archives and Records Management Education and Training in Africa; Challenges and Opportunities,* Pretoria, South Africa, Department of Information Science, University of South Africa.

Kemp, S. (2017) *Digital in 2017: Global Overview,* We are Social. Available at https://wearesocial.com/special-reports/digital-in-2017-global-overview

Luiz, J.M. and Radebe, B. (2012) *The Strategic Location of Regional Headquarters for Multinationals in Africa,* Johannesburg, South Africa, University of the Witwatersrand.

Mbugua, S. (2015) *Challenges Facing Fire Incident's Response in Kenya,* LinkedIn. Available on: https://www.linkedin.com/pulse/challenges-facing-fire-incidents-response-kenya-steve-mbugua/

Millar, L. (Ed) (2009), *Understanding the Context of Electronic Records Management*, London, United Kingdom, International Records Management Trust.

National Disaster Management Authority, NDMA, India (2013) *National Disaster Management Guidelines; Hospital Safety,* New Delhi, Republic of India, NDMA-India.

Ngoepe, M. (2008) *An Exploration of Records Management Trends in the South African Public Sector: A Case Study of the Department of Provincial and Local Government,* Pretoria, South Africa, University of South Africa.

Public Procurement Oversight Authority [PPOA] (2010) Public *Procurement Records Management Procedures Manual*, Nairobi, Kenya, Public Procurement Oversight Authority.

Robinson, N., Graux, H., Parrilli, D.M., Klautzer, L. and Valeri, L. (2011) *Comparative Study on Legislative and Non-Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report*, Cambridge CB4 1YG, United Kingdom, RAND Europe.

Rockefeller Archive Center (2008) *Records Retention and Disposition Guidelines,* New York, United States, Collaborative Electronic Records Project, Rockefeller Archive Center.

Serianu (2016) *Africa Cyber Security Report 2016; Achieving Cyber Security Resilience, Enhancing Visibility and Increasing Awareness*, Nairobi, Kenya, Serianu Limited.

Source8 (2015) *Four Trends Shaping the future of Data Centres in Africa*. Available on:

Symantec (2016) *Cyber Crime and Cyber Security Trends in Africa,*Addis Ababa, Ethiopia,Symantec and African Union Commission.

UNISDR, (2016) *Poverty & Death: Disaster Mortality 1996-2015,*Geneva, Switzerland, The Centre for Research on the Epidemiology of Disasters (CRED)

United Nations Committee for Development Policy, UNCDP (2017) *List of Least Developed Countries; June 2017,*New York, United States, Department of Economic and Social Affairs, Development Policy and Analysis Division.

United Nations Conference on Trade and Development, UNCTAD (2016) *Economic Development in Africa Report 2016; Debt Dynamics and Development Finance in Africa,*Geneva, Switzerland, United Nations Publications, ISBN 978-92-1-112900-7.

United Nations Conference on Trade and Development, UNCTAD, (2016), *Statistical Tables on the Least Developed Countries (LDCs)– 2016,*Geneva, Switzerland, United Nations Publications.

US Department of Education, Privacy Technical Assistance Centre, (2011) *Data Security: Top Threats to Data Protection*. Available on: http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf

Wachira W. and Smith, W.P. (2013) *Major Incidents in Kenya: The Case for Emergency Services Development and Training,* ResearchGate. Available on: https://www.researchgate.net/publication/235415012_Major_Incidents_in_Kenya_the_Case_for_Emergency_Services_Development_and_Training

WikiLeaks (2016) *Ten Years, Ten Million Documents,* Wikileaks.

Xalam Analytics (2015) *The African Data Center Rises Data, Center Colocation, Demand, Supply, Forecasts & Business Models in African Markets*. Available on: http://www.xalamanalytics.com/wp-content/uploads/2016/02/Xalam-Africa-Data-Center-Report-Table-of-Contents.pdf

Yu, P.K. (2015) *Trade Secret Hacking, Online Data Breaches and China's Cyber Threats, Intellectual* Property Law Center, Des Moines, United Sates of America, Drake University Law School.