DISASTER RECOVERY: LEVERAGES THE ADMINISTRATIVE FINESSE OF PUBLIC SECTOR ORGANIZATIONS IN RIVERS STATE, NIGERIA

BRISTOL Marvellous and PROF. E**. TANTUA E. (JNR)**
Department of Office and Information Management, Faculty of Administration and Management, Rivers State University

ABSTRACT

Administrative finesse encompasses the skills, qualities, and strategies employed by administrative professionals to navigate the complexities of their roles effectively. This study examines the relationship between disaster recovery and administrative finesse of public sector organizations in Rivers State, Nigeria. The study was conducted through the review of literature on the concept of the study variables which includes: disaster recovery, administrative finesse, information security and seamless workplace. The reviewed variables demonstrated positive relationship with disaster recovery and administrative finesse with information security and seamless workplace also showing positive results as outcome of administrative finesse. Relying on the result of the study observations, we concluded that, there is significant relationship between disaster recovery and administrative finesse. We therefore, recommended that, public sector organizations should ensure there administrative approach are skill based as it facilitate effective and efficient disaster recovery by providing good information security and seamless workplace.

Keywords: Disaster Recovery, Administrative Finesse, Information Security, Seamless Workplace

INTRODUCTION

Public sector organizations are entities owned and operated by the government at various levels – national, state/provincial, or local. They are established to provide essential goods and services to citizens and fulfil specific public needs that are not adequately addressed by the private sector. Overtime, there has been consistent public outcry over the negligence of public sector organizations to perform effectively and efficiently and recover from disaster when it struck. Furthermore, the sector is basically faced with a lot of issues and challenges but still continue to struggle while playing its role in public sustainability. Disasters, whether natural or human-made, can have devastating impacts on organizations and disrupt their operations. In such critical situations, administrative finesse plays a crucial role in ensuring the effective management of organizational processes, resources, and personnel. Administrative finesse according to Minztsberg (1973) is a set of skills and competencies essential for effective administration. Also, administrative finesse is perceived as a holistic approach to management that encompasses strategic thinking, resource allocation, and interpersonal dynamics (Kotter, 1982). Looking at the scholars submission on the definition of administrative finesse and the important of administration in the management of the organizational resources and its sustainability in the face of crisis depend mostly on effective administration. Administration is the heartbeat of any kind of organizations, be it small or big. As such, the day to day activities of the organizations are perfected by the administrative unit of the organization and the effectiveness of the administrative personnel determines how fast organization recovers from disaster when it occurred.

Disaster recovery is the ability of organization to recover and navigate from the unexpected event that causes a catastrophic situation and prevent organizations from achieving its objectives. The disaster principles were created in the 1970s when the organizational use of computing technology was first becoming pervasive with massive amounts of data generated. Any interruption to computing services resulted in loss of data with financial repercussions. The ability to return to operations quickly without data loss was important to businesses

(Esnard & Sapat, 2014). For this reason, the disaster recovery industry grew in the 1980s and 1990s, along with government regulations that mandated DRPs including a long-term business continuity plan. Regards to this development, the study tends to examine the impact of disaster recovery and administrative finesse of public sector organizations in Rivers State, Nigeria.

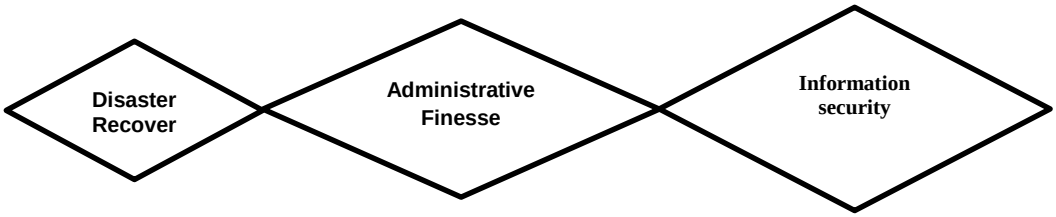

Fig. 1. Conceptual Framework for Disaster Recovery and Administrative Finesse

LITERATURE REVIEW

Theoretical foundation

Contingency Theory: The contingency theory was propounded by Edward Fred Fiedler in 1960. Contingency theory is an approach to organizational structure and design that emphasizes the idea that there is no single, universally effective way to organize a company. Instead, the most appropriate organizational structure and management practices are contingent upon various internal and external factors unique to each organization.

One of the earliest and influential contributions to contingency theory was the work of Burns and Stalker (1961) in their book "The Management of Innovation." They introduced the concepts of "mechanistic" and "organic" organizational structures and argued that the appropriate structure depends on the rate of environmental change. Mechanistic structures, characterized by high levels of formalization, centralization, and specialization, are better suited for stable environments, while organic structures, which are more flexible, decentralized, and adaptive, are more appropriate for dynamic, rapidly changing environments. The central focus of contingency theory is that organizations must adapt their structures, processes, and behaviours to align with the specific circumstances or contingencies they face. These contingencies can include environmental factors (e.g., market conditions, technological changes, industry dynamics), organizational characteristics (e.g., size, strategy, culture), and task or operational requirements (e.g., complexity, uncertainty, interdependence). According to contingency theory, organizations that achieve a proper fit between their internal design and the external environment are more likely to be effective and perform better than those that do not. Consequently, the theory suggests that there is no single, universally optimal organizational structure or management approach; rather, the most effective structure and practices depend on the specific contingencies (situations) faced by the organization. This submission correlates with the popular adage that no one size fit all.

Disaster Recovery: A disaster is a long-term, down time event that can be catastrophic to a business (Nollau, 2009; Habibullah & Baharom, 2010). Disasters are events that have no predictable time line (Paldi et al,2010) and are classified into three types ; Natural, Environmental, or Human/Technological (Omar et al,2011). Nelson (2011) listed the following natural threats: drought, earthquakes, floods, storms , tornadoes, volcanoes, and wildfires. Environmental threats includes: radioactivity, leakages, fires, explosions, rodents, hurricanes and pollution. Human and technological disaster includes: building shutdowns,

sabotage, computer viruses, terrorism, denial of service attacks, trojan worms, software failures, and lack of no knowledge causing catastrophic failure (Nelson, 2011). Failure to communicate within any organization directly affects operations, as does hiring the incorrect personnel for a position, such as those who lack the knowledge or ability to do their job properly (Nelson, 2011; Cox, 2011). Hiring the wrong people can be devastating to a business and may hamper its data restoration efforts (Nelson, 2011). Bad hiring decision lead to theft, embezzlement, workplace violence, and trade secret theft, which trigger a disaster (Philips, 2009). The downtime caused by a disaster event test a DRPs usefulness (Knox, 2012) , and business must recognize they are vulnerable in the event of a disaster and design a DRP that minimizes the failure (Omar et al; 2011).

The aftermath of the earthquake on January 15,1995, in Kobe, Japan, provided an example of corporate dependence on information technology and information systems. The earthquake devasted the region and brought business to a halt (Chang, 2010). Toyota was affected because it relied on technology and it is just-in-time inventory system. The devastation reached across the globe affecting companies in other countries. IBM in the United State, for example, was impacted because Japanese suppliers of memory chips and other computer parts were shut down. None of these organizations had efficient or effective DRPs at the time (Chang, 2010). This was important because there was direct inverse relationship between disasters and business economics (Paldi et al., 2010). Paldi et al. 2010 reviewed the relationship between economic development, education and population in 15 Asian countries between 1997and 2005 and found that the relationship between economic development and disaster loss was nonlinear. In general, lower-income countries were disaster resilient, whereas higher-income countries experienced more disasters but faster recovery. Also, the higher the level of education in a country and the larger it's land area, the lower it number of disaster-related fatalities. Countries with higher incomes had better recovery options than poorer countries. Developing countries were affected most, having the highest rates of death and poverty after a disaster (Paldi et al., 2010). Dependence on a central authority that was not responsive to Preparedness and communication failures, meanwhile, decreased predisaster responsiveness especially in developing countries (Nollau, 2009).

Classical disaster recovery, which established roots in emergency and disaster management, typically included four components: Mitigation, preparedness, response and recovery (Esnard & Sapat, 2014). In this model, there was no performance measurement designed to reduce or eliminate the risk from disaster. Preparedness meant the overall ability or readiness to respond to emergencies or crises, Response referred to the action taken to prevent further damage in a an emergency, and Recovery referred to the ability to return to normal operations including any reconstruction or rebuilding (Esnard & Sapat, 2014). When organization created a DRP, they used all four components to ensure that a business returned to operations within a reasonable amount of time. One of the potential issues, however, was whether the data backup portion of such an operation was viable.

Disaster recovery plans (DRPs) helps organization return to their formal level of productivity (Nollau, 2009) following a disaster. Business leaders often assume that DRPs were designed for large corporations' disaster planning, but smaller companies need to engage in disaster planning as well (Guy & Lownes-Jackson,2010). Nollau (2009) explained that the ability to operate in an alternative manner was crucial to increasing the probability that a business will remain open after a disaster occurs. Although some business have DRPs and data backup plans, they occasionally die not test them. Hurricane Katrina proved to the business world that all business need an effective DRP (Omar, Alijani & Mason, 2011). Organizations should test

their data backup to ensure that they can return to operational status after a disaster (Smith, 2012). Since Hurricane Katrina, many businesses began requiring mandatory monthly testing of data backup and restoration function (Omar et al; 2011).

Why is Disaster Recovery Planning Important

There are several reasons why disaster recovery planning is essential for any organization that relies on IT infrastructure to carry out it's operations.

Minimizes Downtime Losses: Disaster can cause significant downtime for an organization which can results in loss of revenue and productivity. A well-designed disaster recovery can minimize downtime by ensuring that critical systems and applications are restored as quickly as possible. This can help an organization to recover more quickly from a disaster and reduce the impact on its business operations.

Ensure Business Continuity: Disaster recovery planning is an important component of an overall business continuity plan that seeks to ensure that an organization can continue to operate in the event of disaster. By having a disaster recovery plan in place, an organization can ensure that critical business functions are restored as quickly as possible, minimizing the impact of the disaster on its operations.

Protects Critical Data: In today's digital age data is one of the most valuable assets that an organization has. A disaster cam result in the loss of critical data, which can be devastating for an organization. A disaster recovery plan can help to protect critical data by ensuring that it is back up and can be restored in the event of a disaster.

Enhance Security: Disasters such as cyberattacks can have a significant impact on an organization's IT infrastructure. A disaster recovery plan can help to enhance security by ensuring that critical systems and data are protected and can be restored in the event of a cyber attack.

Ensures Compliance: Many organizations are subject to regulations and compliance requirements that require them to have a disaster recovery plan in place. Failure to comply with these requirements can result in significant times and other penalties. By having a disaster recovery plan in place, an organization can ensure that it is in compliance with these regulations and avoid potential penalties.

Administrative Finesse: In the realm of organizational management, the concept of "administrative finesse" has emerged as a critical factor influencing the success and efficiency of administrative processes. Administrative finesse encompasses the skills, qualities, and strategies employed by administrative professionals to navigate the complexities of their roles effectively. Administrative finesse can be defined as the ability to navigate and manage administrative tasks with dexterity, efficiency, and finesse (Brown & Duguid, 1991). It involves a deep understanding of organizational processes, policies, and procedures, as well as the ability to anticipate and proactively address potential challenges or bottlenecks (Mintzberg, 1975). Individuals with administrative finesse possess a unique combination of technical skills, interpersonal abilities, and strategic thinking. Administrative professionals with finesse possess a comprehensive understanding of the organization's goals, strategies, and internal dynamics (Strati, 1999). They can anticipate potential challenges, identify

opportunities for improvement, and align administrative tasks with broader organizational objectives (Mintzberg, 1975).

This strategic mindset enables them to prioritize effectively, allocate resources efficiently, and contribute to the overall success of the organization. Administrative finesse involves the ability to communicate clearly, concisely, and persuasively with individuals at all levels of the organization (Strati, 1999). Strong interpersonal skills facilitate collaboration, problem-solving, and conflict resolution, enabling administrative professionals to build and maintain positive working relationships (Brown & Duguid, 1991). Administrative finesse requires adaptability and resilience to navigate these demands effectively (Mintzberg, 1975). Individuals with finesse can quickly adjust to changing circumstances, remain composed under pressure, and maintain a solutions-oriented approach to problem-solving (Strati, 1999). This adaptability and resilience contribute to the overall efficiency and effectiveness of administrative processes.

In today's rapidly evolving technological landscape, administrative finesse encompasses the ability to leverage technology effectively and optimize processes (Brown & Duguid, 1991). Administrative professionals with finesse are adept at adopting and utilizing various software, tools, and platforms to streamline administrative tasks, improve productivity, and enhance collaboration (Strati, 1999). They continuously seek opportunities to refine and improve existing processes, ensuring efficiency and alignment with organizational objectives. Administrative finesse is not a static attribute but rather a continuous journey of growth and development. Individuals with finesse recognize the importance of professional development and continuous learning (Brown & Duguid, 1991). They actively seek opportunities to enhance their skills, stay updated with industry trends, and expand their knowledge base (Strati, 1999). This commitment to lifelong learning ensures that administrative professionals maintain their finesse and remain valuable assets to their organizations. It has a profound impact on organizational performance. Individuals with finesse contribute to improved operational efficiency, enhanced communication and collaboration, and increased productivity (Mintzberg, 1975). Their strategic mindset and ability to anticipate and address challenges proactively can lead to cost savings and improved resource allocation (Strati, 1999). Furthermore, administrative professionals with finesse often serve as valuable partners to decision-makers, providing insights and recommendations that support informed decision-making processes (Brown & Duguid, 1991).

Information Security: The recent classification of information as one top asset of the organization sees organizational information consistently been under serious attack from internal and external members of the organization. In the event of this scenario, organizational leaders are constantly advice to ensure the security of its information. Information security is defined as defensive mechanism put in place by organization to protect and prevent unauthorized individuals from gaining access to organization information. The competitive nature of business necessitated the proper security of organizational efficiency information or database, loosing vital information to the competitors or thief can result to total collapse of the organization. The increase in knowledge and information technology and its numerous users (both good and bad) of information system has been one of the major problems operating business on the internet despite it numerous advantages (Schlienger & Teufel, 2003).

According to Singh (2009) secured information must obey basic and sensitive properties called the triad of information security. One of which is information confidentiality. Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. In general, Security is the quality or state of being secured from

unauthorized users of the information system, or to be free from danger (Xuemei, Yam & Lixing, 2009). It is the protection of organizational assets (digital asset) against adversaries, from those who would do harm, intentionally or otherwise. For example, it is the objective of the National security of a state to protect its citizenry from any external attack or harm (Mathisen, 2010). The security department protect the sovereignty of a state, it's assets, it's resources, and it people. Achieving the appropriate level of security for an organization also requires a multifaceted system, the software, the hardware and the user cooperative to achieve the same goal (Bazzina, 2006).

For an information system to be successful, the following multiple layers of security is put in place to protect its operations;

1. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse
2. Personnel security, to protect the individual or group of individuals who are authorized access to the organization and its operations.
3. Operation security, to protect the details of a particular operation or series of activities.
4. Communication security, to protect communication media, technology, and content.
5. Network security, to protect networking components, connections, and contents.
6. Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

Seamless Workplace: The concept of the seamless workplace has garnered significant attention in recent years as organizations strive to adapt to the rapidly evolving digital landscape and changing workforce dynamics. This paradigm shifts challenges traditional organizational boundaries and hierarchies, fostering a more fluid, collaborative, and technology-enabled work environment. The Seamless Workplace is characterized by a blurring of boundaries between physical and virtual spaces, enabling employees to work seamlessly across different locations, devices, and platforms (Millard & Ross, 2006). It represents a shift from the traditional office-centric model to a more flexible and distributed approach to work (Gratton, 2011). According to Khanna and New (2008), the Seamless Workplace is an environment where people can work together effectively, regardless of their physical location, using whatever tools and processes are most appropriate for the task at hand. Also the emergence of the seamless workplace is primarily driven by advancements in digital technologies and communication tools. Cloud computing, virtual collaboration platforms, and mobile devices have enabled employees to access information, collaborate, and work remotely with relative ease (Landers, 2015). As Millar et al. (2018) argue, "the proliferation of new technologies has enabled the development of new forms of distributed and remote working, allowing for greater flexibility and mobility in where and when work is carried out".

Furthermore, the seamless workplace is also shaped by changing employee expectations and organizational cultures. Younger generations, such as millennials and Generation Z, have grown up with digital technologies and value flexibility, work-life integration, and collaboration (Gratton, 2011; Meister & Willyerd, 2010). Organizations are responding to these shifting expectations by adopting more flexible and seamless work arrangements to attract and retain top talent (Cisco, 2011). Tools such as video conferencing, instant messaging, and collaborative document editing enable teams to work together seamlessly across geographical boundaries (Landers, 2015; Malhotra et al., 2007). However, as Intindola et al. (2021) highlight, successful virtual collaboration requires "developing norms, routines,

and technologies that facilitate communication, coordination, and cooperation among distributed teams".

Moreover, a seamless workplace often requires a significant cultural shift within organizations. Leaders play a crucial role in fostering a culture of trust, empowerment, and accountability (Gratton, 2011; Landers, 2015). As Millar et al. (2018) suggest successful implementation of the seamless workplace requires a change in mindset and culture, with a focus on outcomes rather than physical presence. The physical workspace is also evolving to support the Seamless Workplace paradigm. Open floor plans, huddle rooms, and activity-based working arrangements are designed to facilitate collaboration, focused work, and seamless transitions between physical and virtual environments (Gratton, 2011; Waber et al., 2014). Additionally, the integration of smart technologies, such as sensors and Internet of Things (IoT) devices, is enabling the creation of intelligent workspaces that adapt to user needs and preferences (Cisco, 2011; Millar et al., 2018). Seamless Workplace offers increased flexibility and autonomy, it also presents challenges related to work-life balance and employee well-being. As boundaries between work and personal life blur, employees may experience increased stress, burnout, and difficulty disconnecting from work (Landers, 2015; Millar et al., 2018). Organizations must proactively address these concerns by implementing policies, training, and support systems to foster a healthy work-life integration (Gratton, 2011; Intindola et al., 2021). The seamless workplace has implications for talent management and workforce mobility. With the ability to work from anywhere, organizations can access a global talent pool and leverage remote workers or virtual teams (Khanna & New, 2008; Landers, 2015). However, this also requires adapting recruitment, on boarding, and performance management processes to accommodate distributed and mobile workforces (Gratton, 2011; Millar et al., 2018).

CONCLUSION

Disaster is something that no one plan for or expected to occur. As the name implies, disaster is any unexpected event that prevent organization from achieving objective as well as incurring loss of assets to organization. The ability of organization to recover it assets from disaster depend largely on the administrative finesse of the organization. It encompasses a range of skills, qualities, and strategies essential for effective administration. It involves organizational awareness, strategic thinking, interpersonal skills, adaptability, resilience, technological proficiency, and a commitment to continuous learning. Through effective administrative finesse, organizations can enhance operational efficiency, improve communication and collaboration, and ultimately drive better organizational performance. As administrative roles continue to evolve and become increasingly complex, the value of administrative finesse will only become more pronounced. This study has demonstrated that, organization with effective administrative finesse have the ability to bounce back from disaster when they occur, hence the needs for administrative unit of organization to be skilful and functional.

RECOMMENDATION

We recommended that, public sector organizations should ensure their administrative approach are skill based as it facilitate effective and efficient disaster recovery by providing good information security and seamless workplace.

REFERENCES

Abadi, D. J. (2009). Data management in the cloud: Limitations and opportunities. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, IEEE.

Aggelinos, G. & Katsikas, S. K. (2011). Enhancing SSADM with disaster recovery plan activities. *Information Management and Computer Security, 19*(4), 248-261.

Al-Badi, A., Ashrafi, R., Al-Majeeni, A., & Mayhew, P. (2009). IT disaster recovery: Oman and cyclone Gonu lessons learned. *Information Management & Computer Security, 17*(2), 114-125.

Bazzina, M. (2006). *Security standard and support system report. A collaborative project review*, the Commonwealth Attorney-General's department and standards Australia. NSW: Standard International.

Beggan, D. M. (2011). Disaster recovery considerations for academic institutions. *Disaster Prevention and Management, 20*(4), 413-422.

Bjorck F (2001). *Security Scandinavian style: Interpreting the practice of managing information security in Organisations*. Licentiate Thesis, Department of computer and systems sciences, Stockholm University/Royal institute of technology, Stockholm.

Boyd, A., Chambers, N., French, S., & King, R. (2014). *A scoping study of emergency Planning and management in health care: What further research is needed?* Manchester, England: National Institute for Health Research. Retrieved from http://www.netscc.ac.uk/hsdr/files/project/SDO_FR_09-1005-01_V01.pdf

Chang, S. E. (2010). Urban disaster recovery: A measurement framework and its application to the 1995 Kobe earthquake. *Disasters Prevention and Management, 34*(2), 303-327.

Cox, R. S. (2011). Like a fish out of water: Reconsidering disaster recovery and the role of place and social capital in community disaster resilience. *American Journal of Community Psychology, 43*(3-4), 395-411.

Cisco. (2011). *The seamless workplace: Future of work.* Cisco Internet Business Solutions Group.

EC-Council. (2011). *Disaster recovery.* Clifton Park, NY: Cengage Learning.

Egli, D. S. (2013). Beyond the storms: Strengthening preparedness, response, and Resilience in the 21st century. *Journal of Strategic Security, 6*(2), 32-45.

Engemann, K. J., & Henderson, D. M. (2012). *Business continuity and risk management*. Brookfield, CT: Rosthsteiin Associates Incorporated.

Esnard, A. M., & Sapat, A. (2014). *Displaced by disaster: Recover and resilience in a Globalizing world. Environmental crises, population displacement, and disaster Recovery.* New York, NY: Routledg

Guster, D. C. (2012). Outsourcing and replication considerations in disaster recovery Planning. *Disaster Prevention and Management, 21*(2), 172-183.

Guy, R., & Lownes-Jackson, M. (2010). *Business continuity strategies: An Assessment of planning, preparedness, response and recovery activities for Emergency disasters.* IHart,13,87-97. Retrieved from http://eds.b.ebscohost.com.ezp.waldenulibrary.org/eds/pdfviewer/pdfviewer?vid=2&a mp;sid=6c5a6b62-aac1-4a94-93fa-5ee0423b8df6%40sessionmgr102

Gratton, L. (2011). *The shift: The future of work is already here.* Harper Collins.

Intindola, M. L., Jacobsberg, L. B., & Mathwick, C. (2021). Virtuality in the workplace: A systematic literature review. *International Journal of Management Reviews, 23*(3), 325-348.

Kadlec, C., & Shropshire, J. (2010). Best practices in IT disaster recovery planning among US banks. *Journal of Internet Banking and Commerce, 15*(1), 1-11.

Karim, A. (2011). Business disaster preparedness: An empirical study for measuring the factors of business continuity to face business disaster. *Internal Journal of Business and Social Science, 2*(18), 183-192.

Knox, K. (2012). *Improve your IT disaster recovery plan and your ability to recover from a disaster*. Gartner, Inc.,

Khanna, P., & New, J. (2008). *Removing the boundaries: The seamless workplace*. Cisco Internet Business Solutions Group.

Kotter, J. P. (1982). *The general managers.* Free Press.

Landers, R. N. (2015). Computing intra-individual processes: Introduction to the special issue, *Journal of Management, 41*(4), 855-857.

Malhotra, A., Majchrzak, A., & Rosen, B. (2007). Leading virtual teams. *Academy of Management Perspectives, 21*(1), 60-70.

Meister, J. C., & Willyerd, K. (2010). *The 2020 workplace: How innovative companies attract, develop, and keep tomorrow's employees today.* HarperCollins.

Millard, D., & Ross, M. (2006). Web 2.0: Hypertext by any other name? *In Proceedings of the Seventeenth Conference on Hypertext and Hypermedia (pp. 27-30). ACM.*

Millar, J., Aiken, M., & Chuvakin, A. (2018). *The seamless workplace: Driving digital transformation with mobile cloud technologies.* Aruba Networks.

Mathisen, J. (2010). *Measuring information security awareness- a survey showing the Norwegian way to do it*. Master's Thesis, Gjovik University College.

Mintzberg, H. (1973). The nature of managerial work. Harper & Row.

Nelson, S. (2011). *Pro data backup and recovery.* New York, NY: Springer.

Nollau, B. (2009). Disaster recovery and business continuity. *Journal of GXP Compliance, 13*(3), 51-58.

Omar, A., Alijani, D., & Mason, R. (2011). Information technology disaster recovery Plan: Case study. *Academy of Strategic Management Journal, 10*(2), 127-141.

Paldi, J., Habibullah, M., & Baharom, A. H. (2010). Economic impact of natural disasters Fatalities. *International Journal of Social Economics, 37*(6), 429-441.

Phillips, B. (2009). *Disaster recovery*. Boca Raton, FL: Auerbach Publications

Rahman, B. A. (2012). Issues of disaster management preparedness: A case study of Directive 20 of national security council Malaysia. *International Journal of Business and Social Science, 3*(5). 135 -146

Schlienger, T and Teufel, S. (2003). *Analyzing information security culture: Increased trust by an appropriate information security culture in Database and Expert systems applications, Proceedings.* 14 th International workshop, 405-409

Singh, S (2009). *Database system: Concepts, design and applications.* New Delhi: Pearson Education India

Smith, G. (2012). *Planning for post-disaster recovery: A review of the United States Disaster assistance framework.* Washington, D.C.: Island Press.

Toigo, J. (2013). *Disaster recovery planning: Getting to business-savvy business Continuity.* Upper Saddle River, NJ: Prentice Hall

Thelen, P. (2020). Virtual officing and the covid-19 pandemic: Transitioning to permanent remote work. *The Scholar, 22*(1), 1-7.

Waber, B., Magnolfi, J., & Lindsay, G. (2014). Workspaces that move people. *Harvard Business Review, 92*(10), 68-77.

Xuemei, L., Yan, L., and Lixing, D. (2009). 'Study on information security of industry management'. *In information processing*, APCIP, Asia-Pacific Conference, 522-524.