An Empirical Evaluation of Information Technology related Disaster Recovery Readiness in Ghanaian Universities.

[1]Jojo Desmond Lartey, [2]Paul Asante Danquah & [3]James Anani Amezi
[1,2 & 3] Department of Information Technology
Heritage Christian College
Accra, Ghana.
E-mail: danquahpaul@gmail.com

ABSTRACT

Universities are increasingly reliant on information technology in teaching, learning and research. In any institution, students' data and other corporate information form a critical and valuable asset of the organization. Disaster recovery planning is expected to protect the information against any form of loss. This research focused on investigating the disaster recovery readiness and attitude of universities within Ghana. This research focused on investigating the disaster recovery readiness and attitude of universities within Ghana. Emphasis was on the preparedness of the universities' staff for recovery from information technology disaster. A combination of quantitative and qualitative research approaches were used with emphasis on data collection about disaster recovery related accidents, skill, documentation and routine activities. The originality of this research is in the data collected from the universities and used as a basis for conclusion. The results showed that most universities in Ghana are fundamentally ill-prepared for information technology disasters. It needs to be noted that the results may not be suitable for generalization since only 26 out of 97 universities were researched.

Keywords: Ghanaian Universities, Disaster Recovery Readiness

CISDI Journal Reference Format
Jojo Desmond Lartey, Paul Asante Danquah & James Anani Amezi. (2019): An Empirical Evaluation of Information Technology related Disaster Recovery readiness in Ghanaian Universities.. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 10 No 3, Pp 65-76.. Available online at www.cisdijournal.org. DOI Affix - https://doi.org/ 10.22624/AIMS/CISDI/V10N3P6

1. INTRODUCTION

Disaster recovery (DR) involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. It is an important factor in continuous Information Technology (IT) system operations. Computerized data is critical to the survival of most organizations that rely on computerized systems to perform daily operations and assist in the decision making process. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events (DRI International, 2017). Disaster recovery is therefore a subset of business continuity. Disaster recovery (BC/DR) has become an essential business strategy which makes up part of the best practices for organizations today, it has grown at a rapid pace and still continues to grow. In light of terrorism, power blackouts, malicious hacking, geopolitical tension, natural catastrophes, fire, organized or deliberate disruptions, system and/or equipment failures, human error, computer viruses, legal issues and workers' strikes.

Others include the security and resilience of an organization's infrastructure have become a day-to-day concern for businesses and management. With this rise in information technology and the reliance on business-critical data, the landscape has changed in recent years in favor of protecting irreplaceable data.
This is especially evident in information technology, with most large computer systems backing up digital information to limit data loss and to aid data recovery.

1.1 Objectives of the research

This study investigates disaster readiness and awareness in Ghanaian universities, considered as organizations which critically depend on IT for business delivery. Readiness and awareness of eminent danger of IT disaster would manifest in attitudes and disposition in the organization, especially in those staff whose job roles make use of IT infrastructure. Rationally therefore, the organization's proactive measure or plan to counter disaster is indicative of its preparedness to avert any possible IT disaster. Consequently, a relationship between readiness, attitudes and disaster proactive plan an organization has is indicative of its resilience to possible IT disaster (Watters, 2014). The question this investigation attempts to answer, therefore, is whether Ghanaian Universities as business organizations, have requisite readiness and attitudes to make them resilient in the face of IT disaster. This investigation hypothesizes that Ghanaian University institutional counter disaster preparedness and attitude has no significant relationship with their proactive plan in place.

The general objective of the research was to investigate the strategies and plans available in the universities to recover from Information Technology (IT) disaster and the preparedness of its staff in recovering from IT disaster. To achieve the objectives, the research addressed the following specific issues:

- Evaluate the universities' disaster recovery strategies and plans.
- Assess the universities' preparedness to recover from IT disaster
- Investigate the adequacy of backup systems and plans necessary to restore provisions to ensure the availability of information required to resume processing.

2. LITERATURE REVIEW

Alawanthan, Dorasamy & Raman (2017) posited that there is a noteworthy research gap perceived on Knowledge Management (KM) in the outlook of Disaster Recovery (DR) in Information Technology (IT) organizations. As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. For example, of companies that had a major loss of business data, 43% never reopen and 29% close within two years. As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event (FEMA,2017).

Nieles, Depsey, & Pillitteri (2017), concede that not all threats are deliberate or adversarial. They identify some non-adversarial threats as errors and omissions, loss of physical and infrastructure support and impacts of personal privacy of information sharing. Nieles, Depsey, & Pillitteri (2017), further explain that information security is a continuous process of management and monitoring in order to protect confidentiality, integrity and availability of information and to ensure quick identification and resolution of evolving threats and vulnerabilities. They explain that though privacy was initially considered to be unrelated to information security, it has an important symbiotic relationship with information security: privacy cannot be assured without information security.

Yang, Yuan & Huang (2015) instructively noted that disaster recovery sites are an important mechanism in continuous IT system operations. Such mechanisms can sustain IT availability and reduce business losses during natural or human-made disasters. Monitoring, as opposed to auditing, involves more than just periodic or constant monitoring of audit logs but also includes traffic and trend analysis, penetration testing, facilities monitoring, intrusion detection, keystroke monitoring and violation processing (Miller & Gregory, 2012).

It is also recognized that even for small multiuser systems, the manual monitoring or review of security features may require significant resources. Employing the use of both active and passive automated tools makes it possible to monitor and review even large systems for numerous security flaws. Some examples of such automated tools are malicious code scanners, host-based intrusion detection systems, checksum functions, system performance monitoring tools, integrity verification programs and password strength checkers (Miller & Gregory, 2012). Disaster recovery planning protects data against loss. If an organization fails to exercise this due care, it could face civil or criminal lawsuits if a preventable disaster destroys important information (Gregory, 2008). The objectives of the DRP includes protecting an organization from major computer services failure, minimizing the risk to the organization from delays in providing services, guaranteeing the reliability of standby systems through testing and simulation, and minimizing the decision making required by personnel during a disaster (Krutz and Vines, 2007).

Disaster Recovery Planning(DRP): Disaster Recovery (DR) is the process an organization uses to recover access to its software, data, network and hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans (Krutz and Vines, 2007). Loss and Data Loss: According to report by Toigo (2002), more than 10 days of computer outage cannot be recovered by most companies. Fifty percent of them go out of business within 5 years if they had outages for that long. Disasters and Other Disruptive Events: These events may require action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files. Therefore, a well-defined, risk-based classification system needs to be in place to determine whether a specific disruptive event requires DRP effect (Schmidt, 2006).

Business Impact Analysis: Business impact analysis (BIA) is a critical step in the development of disaster recovery planning. This involves identifying the various events that could impact the continuity of operations and their financial, human, legal and reputational impacts on the organization. It is the act of proactively strategizing a method to prevent, if possible, and manage the consequences of a disaster, thus limiting the consequences to the extent that a business can absorb the impact. Risk is a dynamic phenomenon, constantly fluctuating due to business activities and market changes hence making it an almost inexact science (Muthukrishnan, 2005). A system's risk ranking involves determining the risk based upon the impact derived from the critical recovery time period and the likelihood that an adverse disruption will occur. Many organizations will use a risk-of-occurrence formula to determine what it deems is a reasonable cost for being prepared. This risk-based analysis process helps prioritize critical systems and develop appropriately scaled recovery strategies. The risk-ranking procedure should be performed in coordination with IS processing and end user personnel.

2.1. Recovery Strategies

The following paragraphs discuss some IT disaster recovery processes.

Hot Site: Gregory (2008) stated that a hot site is a location that is ready to assume production application processing with little or no preparation. Systems, networks, and applications are all in place and up-to-date, and perhaps live data is already on the site or can be loaded up fairly quickly. Generally speaking, a hot site can assume processing with only a few minutes' or hours' notice. Hot Swapping: Hot swapping is the replacement of a hard drive, CD-ROM drive, power supply, or other device with device while the computer system using it remains in operation. The replacement can be due to a device failure or (for storage devices) to substitute other data (Harris 2008). Remote Journaling: Remote journaling allows one to establish journals and journal receivers on the target system that are associated with specific journals and journal receivers on the source system. Once the remote journal function is activated, the source system continuously replicates journal entries to the target system **Danquah**, Aryeetey & Buabeng-Andoh **(2013)**.

Disk Shadowing: Harris (2008) explained that disk shadowing is a technique used to enhance availability and reliability of secondary storage. It consists of dynamically creating and maintaining a set of two or more identical disk images on different disks coupled as a mirrored disk (two disks) or a shadow set (two or more disks). One or more hosts can be connected to a shadow set, which is considered as a single disk device. When a host directs a write request to the shadow set, the data are written to all disks in the shadow set. A read request is executed by reading from any disk in the set.

Warm Site: Warm sites do not involve a main computer, but are partially configured, usually with network connections and selected peripheral equipment (such as disk drives, tape drives, and controllers). The backup equipment involved in warm site recovery must be turned on periodically to receive backups of data from production servers (Hiles, 2007). Cold Site: Cold sites are generally just empty processing centres with little or no networking equipment, and few (if any) systems. Communications facilities may or may not be in place.(Gregory 2008). Hardware and software failures are also identified. System and network hardware on campus is delivered with a set life expectancy, expressed as mean time to failure (MTTF) and mean time to repair (MTTR). Regular preventive maintenance may prolong the life of equipment, but wear, the effects of environmental contamination, and operator errors will eventually lead to the failure of even the sturdiest component. Software failures may result from sources too numerous to count.

2.2 The Ghanaian Context

The national accreditation board for Ghanaian tertiary institutions showed that there a total of 91 degree awarding tertiary institutions in Ghana consisting of 81 private universities and 10 public universities. A research by Akonnor(2007) revealed that disaster recovery plan were virtually non-existent in most Ghanaian Universities, the research showed that risk analysis, flooding, fire, wind, infrastructure outages, hardware and software failures, and sabotage and accidental destruction were identified as potential threats to Ghanaian universities' information systems. Critical records such as council decisions, accounting and financial and payroll information of most universities were not covered in any disaster recovery plan. It was identified, for instance, that soft copies of examination questions corrupted or lost within the last 24 or 48hours to the scheduled time for the paper will mean a retyping of the questions i.e. recoverable at high cost, which may lead to a postponement of the exam paper because of backups.

Danquah, Aryeetey & Buabeng-Andoh(2013) carried out a similar research on disaster recovery in Ghanaian banks and came out with significantly contrary findings;Danquah et al(2013) revealed that there are systems backup and facilities available and personnel who are competent enough to act appropriately to salvage data and restore data when needed.

To this end, staff knowledge on the availability of policy on information security, familiarity with organization's data recovery processes, 'first aid' actions to take in event of identifying huge data losses, and apparently identifying legitimate system disruptions that could cause data integrity to be compromised are adquate.

In view of the above, a similar research eleven years after Akonnor(2007) was be intriguing. Some general recommendations that reflected in both research work are paraphrased below;

1. The organizations should make it a point to have annual or semi-annual reviews of their disaster recovery plans.
2. Human failure or sabotage could be curbed through access control, a feature that runs in many banks but not in universities and does necessarily prevent sabotage from staff.
3. The organizations must develop good information models to ensure that all staff know about the disaster recovery plan and adhere to its dictates and provisions must be strengthened by finding ways of articulation such provisions through simulations or testing or any other means.
4. The staff should be educated or trained on protocols in case of substantial loss in information.
5. The staff should become more proactive in determining malfunctioning of their computer or information systems and take action in time to call for help.
6. The organizations should better publicize emergency numbers that staff could call in case of any disaster. They must also implement strategies and plans to ensure that all staff actually know and understand what to do in cases of disasters.
7. The organizations must increase their investments in data backup and recovery systems through the use of warm and cold sites.
8. The organizations must construct mirror or hot sites or enter into contracts with other relevant parties to provide these services.
9. The administrative structure and authority chain should be designed to support disaster recovery plan in terms of pronouncing information security breaches, giving passes, sanctioning activities, and following recovery processes. In the least, personnel in management should be mandated to follow a certain due protocol in events of disaster.

3. METHODOLOGY

The research used a combination of quantitative and qualitative methods in gathering data. The quantitative method employed was a survey research, a nonexperimental research methodology that ensures data gathering on attitudes, activities, opinions, events and belief, about individuals (Christensen, Johnson & Turner 2015) and organizations were ascertained. Eleven closed ended and nine opened items featured in the 20 questions survey instrument used. The following five attributes, as central elements and construct for DR preparedness, were then generated from closed ended questions: *Accidents*, *Documentation*, "Information ", "Routine"and "Skills" These form a set of variables that elicited "yes" or "no" answers from respondents. The open-ended questions also provided the opportunity for respondents to express themselves freely on their perception of issues. In some situations where responses were unclear, follow-up interviews were done to clarify. These were analyzed both qualitatively and quantitatively to make deductions.

3.1 Study Population, Sampling and Validity

The data was collected from 26 Ghanaian accredited universities out of 97. The research instrument was distributed amongst individuals from different functional units within each university, the functional units were predominantly information technology, accounting, marketing, library and academic faculties.

The categorization was made according to identified job roles relevant to IT DR (Watters, 2014) and thus an appropriate operationalization of the problem being investigated. Specifically 104 questionnaires were distributed with an average of four per institution, a total of 93 were received and used for the analysis. The research instrument was tested in five universities to determine its usability and appropriateness. The positive outcome of the validity test constituted very significant elements that reflect validity of the construct, representative of the DRP being measured by the investigation, given that we had already tested our questionnaire (template attached) and ensured reliability in its content as well as scope for all the stimuli applied to the population participants. Each participant responded, mutually exclusive to "Yes", "No" and "Don't Know" to questionnaire items and the five attributes labelled "ACC ", "Doc", "Info", "Rout" and "Skill" respectively for Accident occurrences; Documentation of disaster plans; Information flow on disaster awareness; Routine maintenance to avert disaster; and Skills training to handle disaster issues or challenges. Thus Attributes (for Counter-Disaster Attributes) and Response (participants response Leve) constituted two categorical variables used in this analysis.

3.2 Data Analysis Procedure

The independent categorical variables were then organized and displayed in the figure 1 bar chart. Inferential statistics, to understand the population, was conducted. R computer programming language was used to run a *Spearman's Chi square statistical test for independence*, for an alpha level of 0.05, to ascertain variability in the two variables. Contingency table was therefore generated for the two sets of variables with "Attributes" as rows and "Responses" as columns. The Chi squared test was considered appropriate given that both variables came from a single population, which in line with the study hypothesis is the need to determine whether there is a significant association or not between these two variables. Test of hypothesis was therefore conducted. Further test – test of association, was carried out to determine the level of association among the variables. All these tests geared towards establishing the strength and direction of relationship between the two variables for the given alpha level of statistical significance.

4. RESULTS

Figure 1 hows a bar chart for attributes against response level in sample subjects.

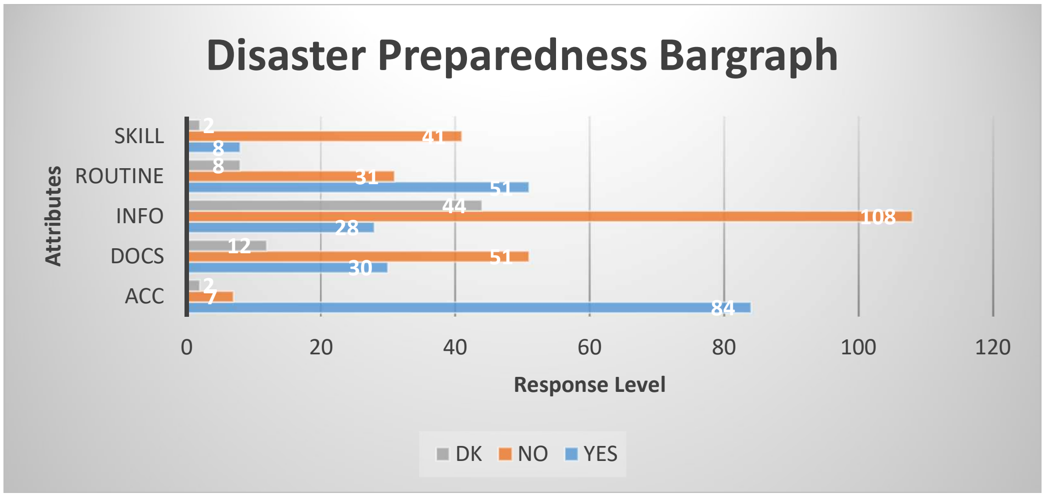

Figure 1: Bar-chart showing level of responses to disaster preparedness attributes

The Chi squared test was carried to accept or otherwise the test of hypothesis of this investigation. The two variables of Attribute and Response levels respectively possess 5 levels and 3 levels.

H_o: Attribute and Response Level are independent.
H_1: Attribute and Response Level are not independent.

The Pearson's Chi-Squared statistics was conducted at a significant level of 0.05 and 8 degrees of freedom, using the R programming language. A X^2- = 187.25, df = 8, p-value < 2.2e-16, respectively for the Chi statistic, degrees of freedom and probability values. Given that the statistical probability value of p=2.2e-16, is much less than our significant level probability of 0.05, the test suggests we reject the null hypothesis, in favour of the alternate hypothesis. This implies that there is a relationship between our categorical variables. Our null hypothesis states that knowing the level of Attribute does not help predict the level of Response. Consequently, this was tested against the alternative hypothesis that knowing the level of Attribute can help predict the level of Response, and thus the suggestion that the variables are related.

The test of association was conducted, as a further test, to determine the nature of relationship and its direction among the two variables. The R programming language was then used to mine this association from the residual and percentage contributions respectively shown in figure 2 and 3. Blue colour signifies positive attraction, and therefore an association between the pair of column and row. Evident from figure 2 is a suggestion for strong association between "Yes" column and "Acc" row while the pairs of "No"/"Skill" , "DK"/"Skill", "Yes"/"Rout" and "No"/"Docs" follow in that order of decreasing positive attraction. The red colours indicate negative residuals, suggesting a repulsion among the pair of variables. Evident from figure 2 is the suggestion that repulsion between pair "No"/"Acc" is the highest, which means a negatively high association between the pair. The least in this repulsion is the pair "No"/"info".

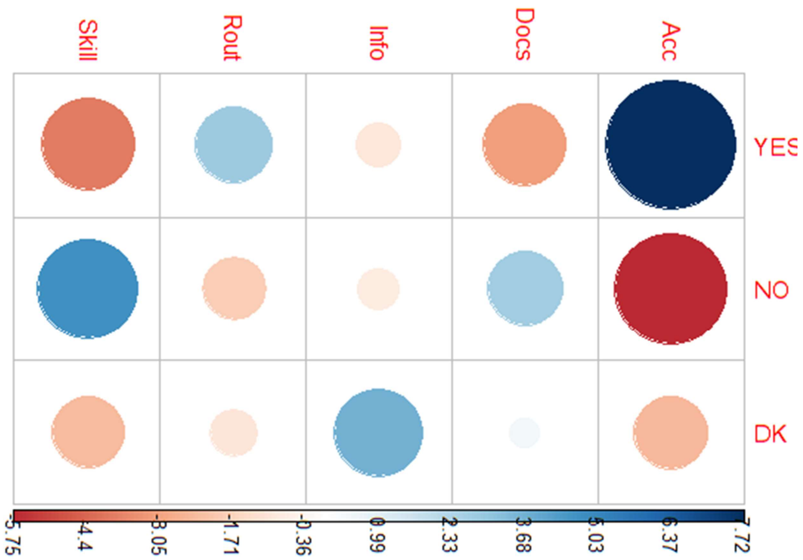

Figure 2: Association between variable levels, with red showing strong association while that of red is strong repulsion. Lighter colours indicate decreasing intensities in respective level of association.

Further analysis of the residual to identify which pairs of the variable levels are responsible for the significance and relationship observed in depicted in figure 3. and again "Acc" contributed most significantly to the observed relationship and association, followed by "Skill", "Docs", "Info" and "Rout" in that order of decreasing contributions.

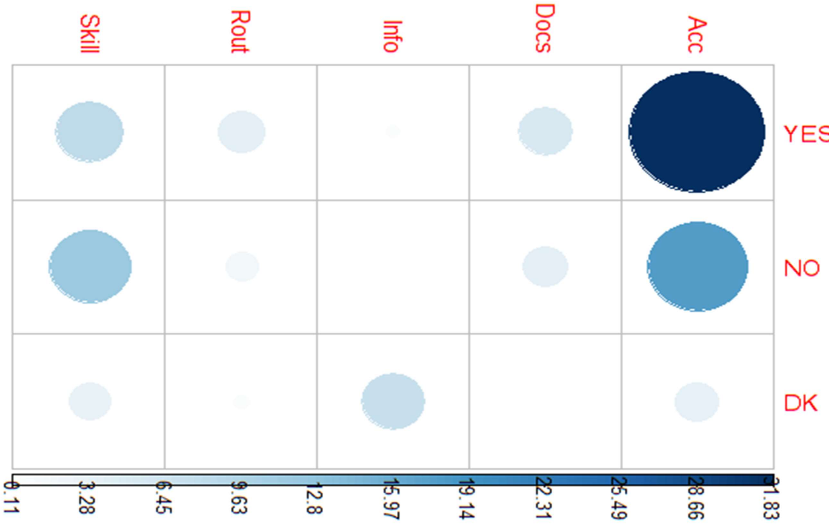

Figure 3: Variables responsible for the direction of relationship and association observed. Intensity of colour suggests level of contribution to the observation

4.1 Qualitative Analysis

Demographics:

Table 1: Distribution of Respondents by University Type

No	University Type	
	Public	Private
	4	22

Table 2: Distribution of Individual Respondents by University Type

No	University Type	
	Public	Private
	13	74

Table 3: Distribution of Respondents by Departments within Universities

	Information Technology	Accounts	Marketing	Administration	Library	Other
	30	10	16	12	10	9

Table 4: Distribution of Respondents by Number of Years of Service at the University

	1 – 5	6 - 10	11 – 15	16 – 20	21 +
	51	31	3	2	0

Responses to open ended questions:

Most people in determining whether a problem with their computers, software, hardware and or networks are defective as to be mentioned as a disaster would at first instance summarily report to the IT department of their various organizations for experts to investigate.

- ❖ The various IT departments in determining whether a problem with their computers are defective as to be mentioned as a disaster would first check to make sure their servers are running effectively at full capacity.
- ❖ The various IT departments in determining whether a problem with their networks are defective as to be mentioned as a disaster would first check to see if computers are still able to communicate with each other at all.
- ❖ The various IT departments in determining whether a problem with their hardware are defective as to be mentioned as a disaster would first check if hardware has not become obsolete.
- ❖ The various IT departments in determining whether a problem with their software are defective as to be mentioned as a disaster would first check if the software at least still works as before after debugging.

A summary of responses to some open ended questions are provided below;

Question: What would you do in case of people (known or unknown) bypassing IS security protocols you are familiar with?

Summary of Responses:
Report to IT
I dont know any security protocol
Shut down firewall
Setup Committee to investigate so action is taken

Question: What do you do when you realize that there is substantial loss of data from your computer or other information equipment (media or print) on your desk?

Summary of Responses:
Report to IT
Report to my supervisor
Backup restoration
Report to management who then setup Committee to investigate so action is taken

Question: In case of disaster, state the information description that you give out to the appropriate contact for action to take place.

Summary of Responses:
Management decide
They give out exact information they cannot find
It depends
Management sets up a committee to investigate and advice on appropriate action
System is down treat this email as very urgent

Question: When do you know that the problems with your computer, software, hardware, network is defective as to mentioned as a disaster?

Summary of responses
when a huge volume of data that is irreplaceable gets lost When they malfunction
When my systems are not behaving the way they should.

Question: What do you do if your colleague's computer is inoperable whereas yours is working?
Summary of Responses A third of respondents will direct the victim to IT staff whereas the rest will make an IT staff look at the problem

Question: How do you know that the integrity of the data you are working with has been compromised?

Summary of Responses:
There is software for detecting like anti-virus
I can't tell
When raw data does not match computerized data
I do not have the capacity to detect
When I can't manipulate it like I use to, because its given me restricted access

Question: How often do you do backups?

Table 5: Summary of Responses

Daily	Weekly	Monthly	Don't Know
3	21	32	31

Local backup done weekly and offshore backup is done monthly

5. FINDINGS AND CONCLUSIONS

1. There is significant relationship between the attributes and the state of preparedness of the population. Accidents contributed strongly to both positive and negative directions in this significance relation observed. Consequently, the alternative hypothesis, favoured in this result, suggests that the knowledge level of Attribute can help predict the level of Response. The implication is that increasing numbers in the population may confirm having experienced some form of disaster. Such prediction level is contra to disaster preparedness, given the positive association. On the other hand, we may also predict that increasing population may experience declining occurrence of accidents, and such prediction level is pro disaster preparedness. The results on this variable is not conclusive, although positive association appears pronounced in the face of dipole contribution to the strength in significant associations observed in the variables. However, intuitively one would expect to have more pronounced negative association predicted in the population to signify counter disaster prepared organisations.

2. Yes, is strongly associated with Accidents, Skill, Docs and Rout in decreasing order. Again, intuitively one would expect reverse in the order of association in these variables since routines maintenance guided by well documented plan and executed by skill personnel make for counter-disaster and may prevent accident occurrences, bring them to barely minimum if not eliminated. The implication is that the studied population appear not mindful of activities needed to prevent disaster as well as inadequately for disaster recovery incidents.

3. No is frequently associated with accidents relatively more than it does with Skills, Docs and Rout in that decreasing order. While this is to be expected, it would be much desirable to have no positive contribution in this direction of association. This also suggest a weakness in preparedness for the population against disaster incidence.

REFERENCES

1. Alawanthan, D., Dorasamy, M., & Raman, M. (2017a, July). Information Technology Disaster Recovery process improvement in organization. In *Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on* (pp. 1-6). IEEE.
2. Alawanthan, D., Dorasamy, M., & Raman, M. (2017b, July). Civic networks, technological and institutional support to build effective disaster preparedness model. In *Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on* (pp. 1-6). IEEE.
3. Christensen, L. B., Johnson, B., & Turner, L. A. (2015). Research methods, design, and analysis, Edinburgh Pearson.
4. Danquah, P. , Aryeetey, S. & Buabeng-Andoh, C.(2013), A Critical Assessment of Information Technology Disaster Recovery Strategies in Ghanaian Banks – *Pentvars Journal* Vol. 7 No. 1,2 &3 pp. 58-75
5. Disaster Recovery Institute (DRI) International (2017)
6. Disaster Recovery and Business Continuity, version 2011. Archived January 11, 2013, at the Wayback Machine. IBM. Retrieved 3 August 2012.
7. Federal Emergency Management Agency (FEMA) Report (2017), Retrieved from: https://www.fema.gov/media-library/assets/documents/134253 (01/10/2018)
8. Gregory, P. H. (2008). IT disaster recovery planning for dummies. Hoboken: Wiley Publishing, Inc.
9. Hiles, A.(2007),The definitive handbook of business continuity management, 2nd Edition, Chichester, England ; Hoboken, NJ : John Wiley & Sons.
10. Klaus, S. (2006), High Availability and Disaster Recovery, Concepts, Design, Implementation, Springer, ISBN 978-3-540-34582-4
11. Krutz, R. L. & Vines, R.D. (2007), The CISSP Prep Guide, Wiley; Gold Edition edition, ISBN-10: 0470307765
12. Miller, L. and Gregory, P.(2012), CISSP For Dummies, 4th Edition, For Dummies, ISBN: 9781118417102
13. Muthukrishnan, R.(2005),The Auditor's Role in Reviewing Business Continuity Planning, ISACA Journal, Volume 4
14. Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security. *NIST Special Publication*, *800*, 12.
15. Secaas Category 9 // BCDR Implementation Guidance CSA, retrieved 14 July 2014.
16. Systems and Operations Continuity: Disaster Recovery. Georgetown University. University Information Services. Retrieved 3 August 2012.
17. Toigo, J. W. (2003). *Disaster recovery planning: Preparing for the unthinkable*. Prentice Hall.
18. Watters, J. (2014). IT Disaster Recovery. In: *Disaster Recovery, Crisis Response, and Business Continuity. Apress, Berkeley, CA*
19. 'What is Business Continuity Management', DRI International, 2017
20. Yang, C. L., Yuan, B. J., & Huang, C. Y. (2015). Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision making method. *Sustainability*, *7*(5), 6149-6188.