USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 3 Number 9 31 DEC 2018

ONOCHIE FAN-OSUALA

A NOTE ON DISASTER RECOVERY[1]

Organizations operate in a risky environment and are often faced with disruptive events and occurrences that can significantly impact their day-to-day operations. These disruptive events and occurrences include cyberattacks, natural disasters, and equipment failures, among others. Organizations must therefore have an overall business continuity plan (BCP) to keep all facets of their business functioning in the midst of disruptions from such negative events. With the increasing dependence of organizations on information technology (IT) systems, organizations must plan for the continuity of business processes which directly rely on IT systems and IT infrastructure in the event of disaster. Business continuity planning covers planning for both information technology (IT) related and non-IT related aspects of a business in the event of disruption. Disaster recovery (DR) is a subset of business continuity, focusing on the information technology and technology systems that support critical business functions. It consists of well-defined plans, strategies, policies, procedures, and actions that describe how to recover or continue the technology infrastructure critical to business operations after a natural or human-induced disaster[2]. During the DR process, organizations recover access to their software, data and/or hardware. The goal is to resume computing capabilities in as little time as possible and to minimize data loss following disruption caused by disaster. The plans, strategies, procedures, and actions that allow organizations to recover from or continue operations after a disaster is called the disaster recovery plan (DRP).

Disaster

Disasters are serious disruptions that are capable of crippling a business or its operations. According to a survey conducted by Forrester research (Dines, 2011) in conjunction with the disaster recovery journal (DSJ), the top causes of business disruption in order are: power failure, IT hardware failure, network failure, winter storm, human error, flood, IT software failure, fire, hurricane, tornado, earthquake, and terrorism.

Classes of Disaster

Although several nuanced classifications of disasters exist, disasters can be classified into two broad categories: natural disasters and man-made disasters (Turner and Pedgeon, 1997).

- **Natural disasters:** are very difficult to prevent and include earthquakes, smog, floods, tornadoes, and hurricanes. They can be very costly to businesses. However, risk management and

[1] Copyright © 2018, *Onochie Fan-Osuala*. This technical note was developed to provide background information in support of one or more case studies published by the *Muma Case Review*. It may be freely copied and shared for non-commercial purposes.

[2] http://www.ibm.com/support/knowledgecenter/SSV2LR/com.ibm.wbpm.admin.doc/topics/cadm_disaster_recovery.html

precautionary measures like avoiding areas prone to such natural disaster and good planning can help as well as lead to the avoidance of significant losses.

- **Man-made disasters**: are the more often occurring form of disasters. They can be intentional (e.g. cyberattacks, bio-terrorism,) or unintentional (disastrous IT bugs, hazardous substance spills, industrial accidents).

Further, the term *technological disaster* has been used to define any disaster that can be in part or entirely attributed to human intent, error, negligence, or involving a failure of a man–made system (Donovan et al, 2014).

From an IT perspective, disruptions or disasters fall into three major groups (Brooks et al, 2002):

- ***Malicious behavior***- bomb threats/ blast, biological and chemical attacks, civil unrest, computer virus, hacking, sabotage, theft, workplace violence, espionage, logic bomb etc.

- ***Infrastructure related*** - burst pipes, blackouts, environmental hazards, power failures, epidemics, evacuations, etc.

- ***Natural disasters***.

Cases of IT Related Disasters

Malicious Behavior: In November 2014, Sony Pictures experienced a cyber-attack that led to the cancellation of the theatrical release of the movie “The Interview”- a comedy about the assassination of the North Korean leader. The cyber-attack essentially wiped clean several internal datacenters of the organization, with confidential information stolen and emails leaked (Granville, 2015). Similarly in September 2014, Home Depot a retailer of home improvement and construction products experienced an attack that compromised about 56 million payment cards of customers and this attack is estimated have cost Home depot about $62 million most of which it spent in credit monitoring.

Infrastructure related: In 1990, an error in a single line of code added during a software upgrade in AT&T caused 75million phone calls to go unanswered across the US (Barker, 2007). The code shut down one of AT&Ts switching centers and caused other switching centers to trip, shut down and reset. This disaster cost American Airline, a business that depended on phone calls for some of its flight reservations about 200,000 reservations. Similarly, in 2007 a malfunction in a piece of inexpensive network card grounded 17,000 airplanes at the Los Angeles International Airport. The problem resulted from the card not shutting down and sending incorrect data across the network of the United States Customs and Border Protection (USCBP) agency bringing the system to a standstill and leading to nobody entering or leaving the US through the airport for eight hours.

Natural Disaster: Hurricane Sandy that affected the eastern coast of the United States in October 2012 took down websites and services like Huffington Post, Buzzfeed and Gawker who had their datacenters in New York costing them significant revenue (Moos, 2012). For Huffington Post, Sandy was a costly and significant experience. Huffington Post had prepared for the 2012 election which was an event that drew a lot of readers to the site for political analysis and opinions. Sandy slammed into New York City eight days before Election Day, bringing down Huffington Post’s data center. Even with three separate datacenters between New York and Newark for failover and redundancies, it took Huffington Post a week to bring things back to normal because Sandy brought all three down (Vance et al, 2012). Similarly in June 2012, severe thunderstorms that hit North Virginia caused Amazon web services (AWS) to lose power and popular websites (Netflix, Instagram, Pinterest) that depend on AWS were affected (Babcock, 2012).

Cost of Disasters

Disasters come at a cost to organizations either in lost time, business, data, etc. It is estimated that as of 2010, the average time to recovery following a disaster was 18.5 hours while on average, businesses lost 4.8 hours' worth of data. Because costs associated with disasters often run into millions (see Exhibit 1), organizations ensure that they identify, quantify, and document these costs during disaster recovery planning.

IT disaster related costs can be broadly classified into four categories (Brooks et al, 2002):

- Employee costs – examples include: idle time as a result of disruption, salaries paid to staff unable to do billable work.
- Direct fiscal losses - examples include: lost revenues as result of downtime, cost of interest on lost cash flow
- Long-term losses – examples include: brand image recovery, penalties from failure, loss of stock value and market share
- Recovery site cost – examples include: cost of replacing infrastructure, software, DR contract activation and support.

Disaster Cycle

The uncertainty in the occurrence of disasters and its attendant negative effects (costs and potential losses) necessitates that organizations devise ways to mitigate these effects. The process by which organizations do this is referred to as the disaster cycle. The disaster cycle is a continuous process in which organization and businesses plan for and reduce potential disaster losses (Partnership for Disaster Resilience, 2007). It consists of four phases:

- **Prevention**: involves identifying and minimizing risks and potential causes of disruption. This include doing routine checks on infrastructure, having redundancy in IT systems and infrastructure, having virus and malware detection systems, fire detection and extinguishing systems, water-sensing alarms, avoiding disaster prone regions when siting offices and datacenters, etc.

- **Preparednes**s: this involves getting ready to cope in the face of a disaster. It includes developing a response and recovery plan, updating and testing the plan, keeping a backup infrastructure or cold site[3] that can maintain key processes and services in the event of a disaster, having disaster insurance coverage etc.

- **Response**: involves activities and actions undertaken when disaster strikes. This involves following established procedures and taking necessary actions, notifying the necessary personnel etc.

[3] Cold-site is one or more data center or office space facilities equipped with sufficient pre-qualified environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations

- **Recovery**: involves getting back to normal. Most organization focus on this phase. It includes restoring the disrupted services or processes, restoring the affected site, salvaging data and information, contacting insurers, analyzing the disaster and improving the disaster plan following the experience.

Although organizations continually iterate through the disaster cycle process, the near certainty of disasters makes the response and recovery phases very critical in this process. Hence, considerable attention is paid to them since they focus on how the organization bounces back or recover from disaster.

Disaster Recovery Strategy (DRS)

DRS is guided by an organization's business continuity plan (BCP) and should indicate key metrics of recovery point objective (RPO[4]) and recovery time objective (RTO[5]) for the organizations business processes. The key metrics are mapped to the underlying IT systems and infrastructure that support organizations' business processes to develop the IT recovery strategy. IT recovery strategy focuses on the IT systems, applications and data that supports the core business processes and includes networks, servers, desktops, laptops, wireless devices, data, and connectivity[6]. Since things will always go wrong and near zero RPOs and RTOs can be very expensive, organizations must set their DRS to acceptable risks.

IT recovery strategies should be developed to prepare for any loss in one or more of the key components of IT systems. These components include:

- IT environment – securing the server and computer rooms, climate control, backup power supply etc.
- Hardware – networks, servers, desktops, laptops, wireless devices, peripherals etc.
- Software –enterprise resource management, email, electronic data interchange, office productivity software etc.
- Data – databases, archives etc.
- Connectivity – fiber, cable, wireless etc.

Disaster Recovery Plan (DRP)

Disaster recovery planning is essential to organizations as it not only mitigates or eliminates threats, but also leads to cost savings (Shreve and Kelman, 2014). Indeed, a disaster recovery guide (Partnership for Disaster Resilience, 2007 p 1) states that every $1 spent on hazard mitigation like DRPs saves the society $4 in response and recovery costs. DRPs focus on helping organizations bridge disruptions in their IT or technology systems, especially where data, software or hardware has been lost or damaged. Since IT systems requirements and organizations continue to evolve, DRP should be viewed as an ongoing practice rather than a one off affair. Many DRPs focus on the risks within the data center (Brooks et al, 2002) despite IT systems facing a variety of risks that go beyond the data center. DRPs should be designed to encompass risks beyond the data center. They should include such elements as contingencies for coping with the sudden and/or unexpected loss of key personnel or staff and how to recover their data[7], especially those directly engaged with organizational IT or technology systems.

[4] RPO describes that amount of historical or archived data that the organization can afford to lose in a disaster

[5] RTO describes the maximum time the organization can permit for a downtime after a disruption or disaster

[6] See http://www.ready.gov/business/implementation/IT

[7]See http://www.disasterrecovery.org/

Some control measures necessary in disaster recovery planning for threat mitigation and elimination are preventive, detective and corrective control measures. Preventive control measures are aimed at averting the occurrence of disruptive event. Detective measures are aimed at identifying or spotting disruptive events, while corrective measures are aimed fixing or restoring the system after a disruption. Good disaster recovery plans contain these control measures.

Disaster Recovery Planning Process

Disaster recovery planning involves an analysis of business process and continuity needs with a focus on disaster prevention and means of recovery in the event of a disruption. Figure 1 outlines the process.

Stages in developing DRPs:

1. Identify and understand organization's activities and how all of its resources are interconnected.
2. Assess the breadth and depth of organization's vulnerability in every area, including operating procedures, physical space and equipment, data integrity, security holes, and contingency planning.
3. Understand how all levels of the organization would be affected in the event of a disaster through a business impact analysis. Quantify losses both financial and otherwise.
4. Develop short- and long-term recovery plans, including how to return to normal business operations and prioritizing the order of functions that are resumed.
5. Test, consistently maintain, and update the DRP as the business changes.

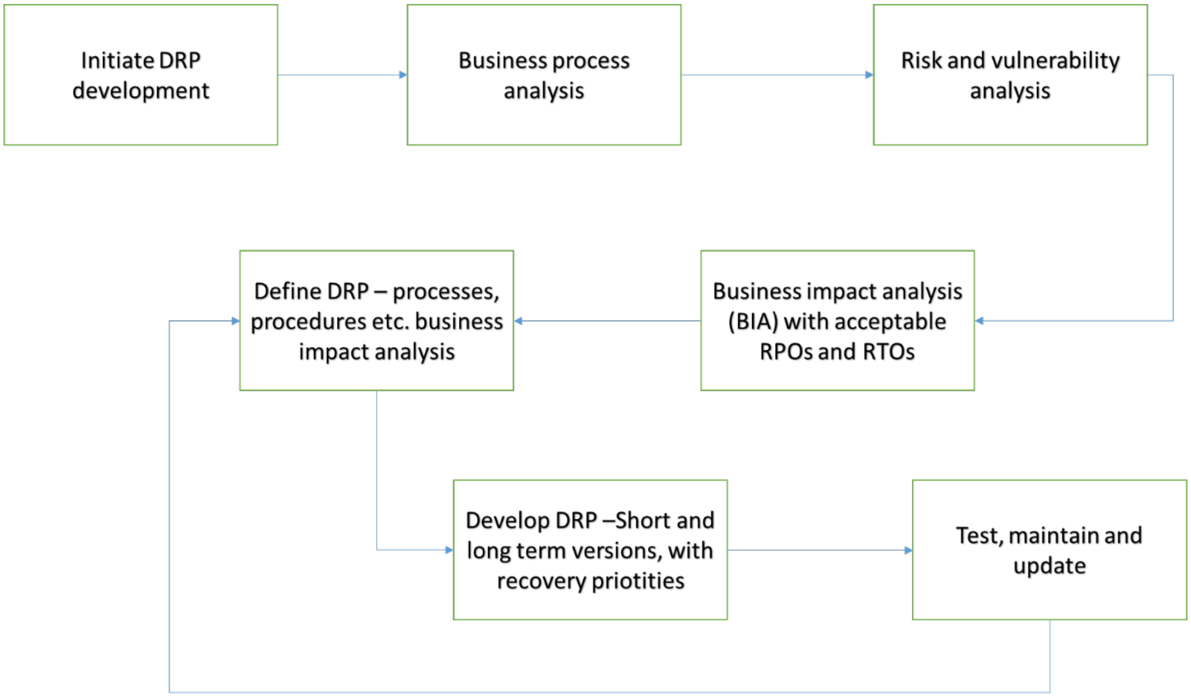

Initiate DRP development
Business process analysis
Risk and vulnerability analysis
Business impact analysis (BIA) with acceptable RPOs and RTOs
Define DRP – processes, procedures etc. business impact analysis
Develop DRP –Short and long term versions, with recovery priotities
Test, maintain and update

Figure 1. Disaster Recovery Planning Process

IT Disaster Recovery Solutions

Since disaster recovery is focused on data recovery and operation restoration time, or service availability, most available DR solutions and implementations focus on data recovery and service availability. These solutions are grouped into 7 tiers and is also used to define an organization's IT disaster recovery readiness and capabilities. SHARE[8] in collaboration with IBM developed the solutions framework. The framework identifies the different tiers and describes each tier in the context of recovery time, cost, and tier characteristics. It can also help organizations determine their current level of disaster recovery solution and what level they may want to achieve. The tier levels are:

1. ***Tier 0 (No off-site data and possibly no recovery)***: organizations in this tier have no saved information, documentation, back up hardware, and contingency plan. These organizations can have unpredictable recovery time or no recovery at all after a disaster.
2. ***Tier 1(Data backup with offsite vaulting)***: organizations in this tier know some of their recovery requirements. They backup and store data at an offsite facility usually by transporting these backups through the pick-up truck access method (PTAM). The offsite locations have no infrastructure to restore data or services and such organizations are prepared to lose several days to weeks of data. Recovery is dependent on when infrastructure is available and typical time for recovery is more than one week.
3. ***Tier 2 (Offsite vaulting with a hotsite[9]):*** This has all the components of Tier 1 with the addition of a hotsite. The hotsite has enough infrastructure to support critical processing requirements. Again PTAM is relied on for the delivery of data. Typical time for recovery is usually more than one day.
4. ***Tier 3 (Electronic Vaulting):*** This tier has all the components of Tier 2, and in addition supports the electronic vaulting of some subset of critical data. Electronic vaulting implies electronically transmitting critical data in a secure off-site location. The electronically vaulted data is typically more current than the transported PTAM data. Typical time for recovery is about one day.
5. ***Tier 4 (Electronic vaulting to hotsites):*** this involves having two active sites with electronic vaulting between them. A processor at the recovery site actively manages the vaulting of data and recovery can be bi-directional. Typical time for recovery is usually up to one day.
6. ***Tier 5 (Two Site, two phase commit with transaction integrity):*** This has all the components of tier 4, and in addition maintain up to date image of primary data center data. Every update on data or transaction is incomplete until it has been written to the secondary site. The two sites are synchronized using high-bandwidth connection between both sites. Typical time for recovery is usually less than 12 hours.
7. ***Tier 6 (Zero data loss):*** This is considered the highest tier of DR and it has infinitesimal to zero data loss. There is immediate and automatic transfer to the secondary site following a disaster. The two sites are synchronized and coupled to allow for automated seamless switchover from one

[8] SHARE Inc. is a volunteer-run user group for IBM mainframe computers that was founded in 1955 by Los Angeles-area users of the IBM 701 computer system.

[9] Hotsite is a data center facility with sufficient hardware, communications interfaces and environmentally controlled space capable of providing relatively immediate backup data processing support.

site to the other when required. It is the most expensive setup to run and typical time for recovery is usually a few minutes.

DR solutions and implementations are cost intensive and often depend on the tier level. Costs associated with DR solutions often come from:

- Running a secondary site with redundant IT infrastructure and systems (staff, software, equipment etc.)
- High bandwidth connections over long distances
- Coupling or clustering management software
- Hardware that support and provides point-in-time volume copies or remote data replication

Conclusion

Disasters are negative disruptive events bound to occur and organizations need to develop strategies to withstand its effects. IT organizations require a strategy or recovery plan that can help them rebound in the face of disasters. Disaster recovery plans (DRPs) are effective in helping bridge and manage disasters. They should be developed around the organization's business continuity needs and should be reviewed frequently since business continuity needs evolve over time.

References

- Babcock, C. (2012). Amazon Outage hits Netflix, Heroku, Pinterest, Instagram. Retrieved from http://www.informationweek.com/cloud/infrastructure-as-a-service/amazon-outage-hits-netflix-heroku-pinterest-instagram/d/d-id/1105148?
- Barker, C. (2007). The Top 10 IT Disasters of all Time. Retrieved from http://www.zdnet.com/article/the-top-10-it-disasters-of-all-time-5000177729/
- Brooks, C., Bedernjal, M., Juran, I., & Merryman, J. (2002). Disaster Recovery Strategies with Tivoli Storage Management. Retrieved from http://www.redbooks.ibm.com/redbooks/pdfs/sg246844.pdf
- Dines, R. (2011). The State of Disaster Recovery Preparedness. Retrieved from http://www.drj.com/images/surveys_pdf/forrester/2011Forrester_survey.pdf
- Donovan, M. Smith, S. Radunovich, H. and Gutter, M. (2014) Impacts of Technological Disasters. Retrieved from http://edis.ifas.ufl.edu/fy1230
- Granville, K. (2015). 9 Recent Cyberattacks Against Big Businesses. Retrieved from http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0
- Moos, J. (2012). Huffington Post, Gawker websites go down as newsrooms lose servers, power. Retrieved from http://www.poynter.org/news/mediawire/193536/huffington-post-buzzfeed-gawker-sites-go-down-as-nyc-feels-effects-of-superstorm-sandy/
- Partnership for Disaster Resilience (2007). Post-Disaster Recovery Planning Forum: How to Guide. Retrieved from http://nws.weather.gov/nthmp/Minutes/oct-nov07/post-disaster_recovery_planning_forum_uo-csc-2.pdf
- Shreve, C.M. and Kelman, I. (2014). Does mitigation save? Reviewing cost-benefit analyses of disaster risk reduction, International Journal of Disaster Risk Reduction, Volume 10, Part A, Pages 213-235,

- Turner, B.A. and Pedgeon, N.F. (1997), Man-Made Disasters, 2nd ed., Butterworth-Heinemann, Oxford.
- Vance, J., Harvey, C., Robb, D., &Maguire, J. (2012). Disaster Recovery: IT Pros Handle Hurricane Sandy. Retrieved from http://www.enterprisestorageforum.com/storage-management/disaster-recovery-it-pros-handle-hurricane-sandy-1.html

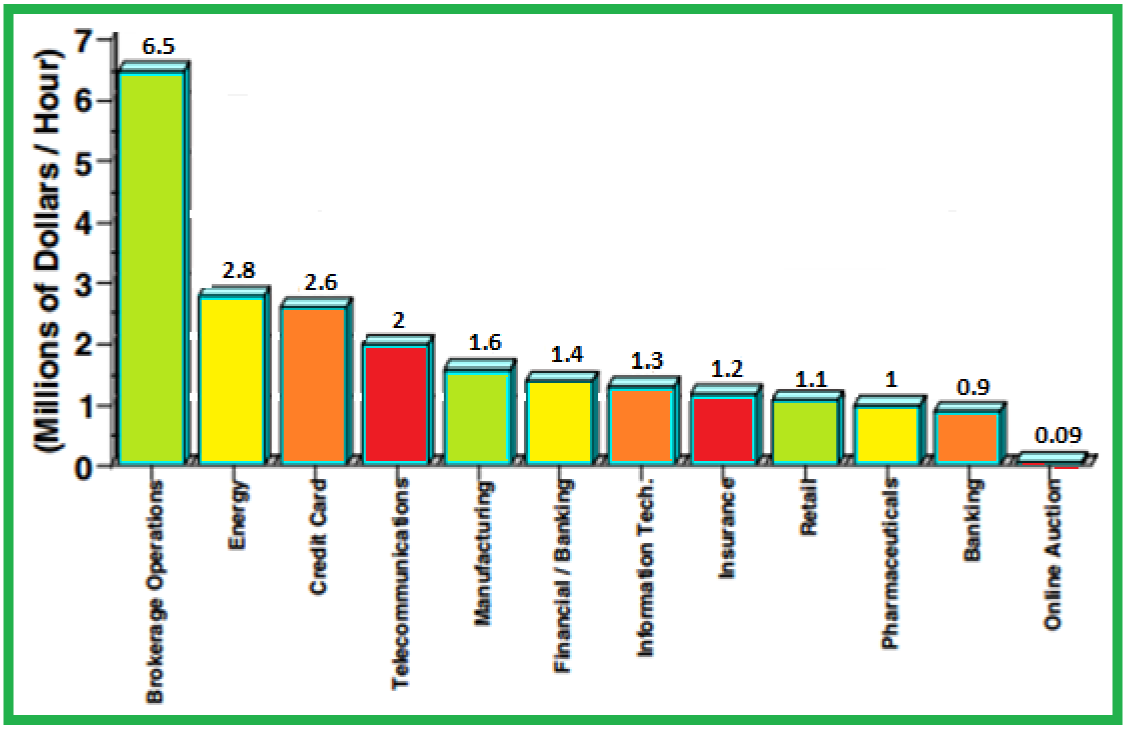
Acknowledgements

Development of this note is based upon work supported by the *National Science Foundation* under Grant No. 1418711.

Biography

Onochie Fan-Osuala is a PhD Candidate in information systems (IS) at the Muma College of Business, University of South Florida. He is interested in using analytics and experimental designs to solve problems bothering on the IS-operations, IS-marketing and IS-entrepreneurship interfaces. His work mostly explore these problems in online platforms and marketplaces.

Exhibit 1: Cost of Disasters



Average cost of downtime for various US industries (adapted from Brooks et al, 2002)