Journal of International Business Education 7: 47-64.
© 2012 NeilsonJournals Publishing.

A Case of Hurricane Irene: Disaster Recovery Preparedness Score

Ehi E. Aimiuwu
Morgan State University, USA

Abstract. This case study is for business students, who are taking a class in Disaster Recovery from an internet securities perspective. It is recommended that the students should have been exposed to the issues of disaster recovery (DR), recovery plans, business criticality, business tolerance, computer security, risk management techniques, and recovery strategies before reading this case. This case is about trying to measure the disaster recovery preparedness (DRP) of a university by creating a disaster recovery preparedness score (DRPS) in order to evaluate how prepared universities are for major disasters that may disrupt their business operations. It also serves as a template for students to understand and appreciate the parts of a complete implementation of a university's DRP plan.

Keywords: disaster recovery, disaster recovery preparedness score, recovery plans, recovery strategy, computer security, risk management techniques.

1. Case Summary

Anna is concerned that Morgan State University (MSU) may not survive the disaster being caused by Hurricane Irene (HI) along the eastern coast of the United States. The damages it has caused in North Carolina along with the numbers of deaths and human displacements have bothered many in the Maryland area. Anna has decided to work with Gary to analyze how prepared MSU is for HI and how quick the school can recover from its damage, if the inevitable occurs. The plan is to come up with a score for measuring DRP for universities based on the four factors that affect DRP, which are risk management techniques, computer security, recovery strategies, and recovery plans. Will MSU survive HI? If it will, how long will it take for MSU to recover from the damage and return to full daily business activity?

2. Case

Anna was fascinated with how quick universities get back on their feet and recover their business processes within hours, days, weeks, months, or even years after a major natural disaster like Hurricane Katrina or the tsunami that hit Japan in March 2011. In late August 2011, HI was advancing destructively towards

Maryland along the east coast, so she interviewed the Vice President of Planning and Information Technology (Joseph Popovich), the Director of Information Technology (Garrett Morgan), the Associate Director of Information Technology (Gary Press), and the Security Engineer of Panning and Information Technology (Wole Akpose) to see how far Morgan State University has come through the years to develop and maintain a disaster recovery plan.

The interview showed how dedicated a university must be towards its customers and their services to them in order to ensure that there is minimum interruption in the business processes. According to them, in order to have a successful disaster recovery plan, a university must analyze the business process, determine the tolerance and criticality of business process, and have a solid recovery plan in place. After speaking with them, Gary chose to work with Anna in regards to how prepared MSU was for HI and DRP.

Based on the discussion with the information technology team, Anna created eight basic qualitative questions, which was based on Fallara (2003), to investigate the disaster recovery preparedness of MSU. The questions where:

1. What specific computer security do you have in place to maintain data confidentiality, integrity, and availability in your network during disaster recovery (DR)? What role will your computer security play in the case of a DR?

2. Do you collect data about IS business processes and how often? How do you collect and store the data?

3. You have levels 1-4 tolerance levels, please give examples of each level and approximately how long the recovery take on an average when DR occurs in each level? How do you measure the criticality and cost at each level during DR?

4. What is the approximate outage time for MSU during DR and how does the down time affect other business processes and resources?

5. Where are your alternate recovery sites (warm, cold, hot, mobile etc)? How often is data stored there?

6. Do you have equipment replacement plan? What kinds of equipments, their function in DR, and how often are they replaced?

7. Do you have DR support teams, how many, what percent of MSU employees are involved, what equipment and functions are they assigned to?

8. Do you do DR training and maintenance of employees and teams, classroom or functional exercise, and how often?

3. The Model

The entire case as well as the model was built around the detailed summary of Fallara (2003). The other references in the case were used basically to emphasize the points and information the paper provided. The model in Figure 1 shows the four factors that affect disaster recovery preparedness, how disaster recovery affects the disaster recovery preparedness score, and ultimately how the disaster recovery preparedness score should be calculated.

The four factors that affect disaster recovery are risk management, computer security, recovery strategies, and recovery plan. The table at the end of the model outlines how the disaster recovery preparedness score (DRPS) should be calculated.

The DRPS should be computed by a business intelligence dashboard and the data should be collected electronically. All data collected towards the DRPS must meet the following criteria:

1. It must be completed annually for employees to understand the importance of disaster recovery.

2. All employees must be involved to emphasize the importance of accurate and complete data entry.

3. Data must be collected in the form of employee surveys and completed electronically for privacy.

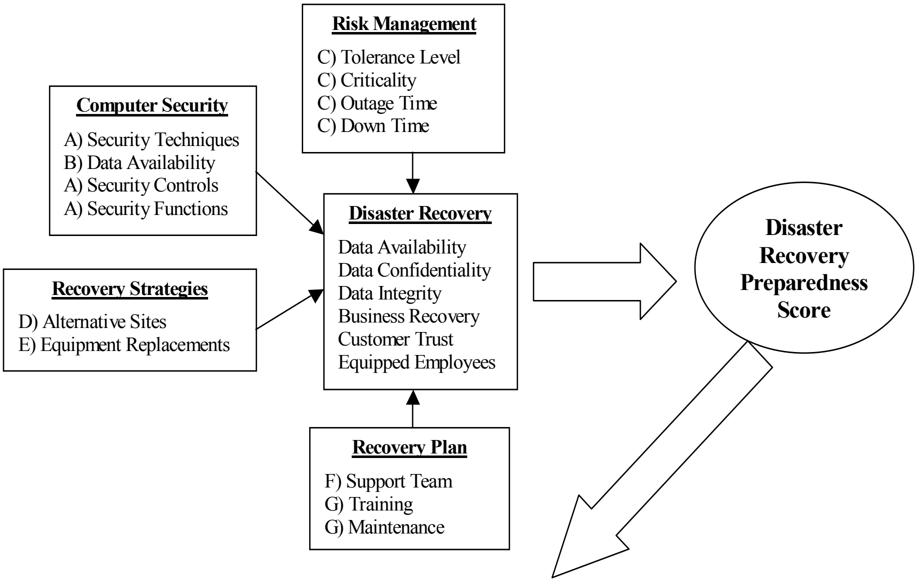
4. All data must be entered into a database for data mining software to analyze and compute (i.e., in the form of a score).

5. Each question for the DRPS must have at least 80% employee approval to get maximum points.

6. DRPS must be displayed on university's homepage to show customers the university's respect for great customer service by making business available, information confidential, and data credible.

For instance, in computing the DRPS for "Letter A" from the Model, if more than 80% of employees who filled the electronic survey believe that the university protects the confidentiality and integrity of every data item entered into the computer system during work, then the university scores a point. If not, they get a zero.

Figure 1: Model of The Factors of Disaster Recovery Preparedness and Their Respective Measurement Points



Letter	Disaster Recovery Preparedness & Points	Total Points
A	Computer Security: Confidentiality & integrity (1)	1
B	Collect business process data (2); Data stored immediately (1)	3
C	Adequate tolerance levels (2); Efficient critical measures (1)	3
D	Alternative recovery site (2); Adequate location of alternative recovery site (1)	3
E	Adequate equipment plan (2); Efficient equipment replacement plan	3
F	Great DR support team with assigned roles (3); Many employees with backup disks & tapes (1)	4
G	Effective DR training & maintenance (2); Frequency of training and maintenance (1)	3
Grand Total	Disaster Recovery Preparedness Score for Universities	20 (100%)

For each question, if fewer than 80% of employees do not agree that the university is adequately meeting the standard, the university gets a zero. It is an all-or- nothing scale, except for the first part of "Letter F". The university gets a point even if less than 80% feel that they are a part of the DR support team, as long as there is a DR support team available in the university. If not, the university gets a zero.

Every employee must know that every second of their work activity is part of a disaster recovery process or plan in terms of data accuracy, data currency, data completeness, and data consistency. Employees not knowing that they are a part of the DR support team are a huge flaw in the disaster recovery preparedness effort of an organization. This is why this section has the highest allocated points in the DRPS. The computer security section (Letter A), has the lowest allocated points because every university is expected to have some form of computer security to even lay the foundation for a DRP plan. The total DRPS is 20 points or 100%.

1. The Student

Anna White is a PhD student in the School of Business at Morgan State University in Baltimore, and she is concentrating in Information Sciences and Systems. Anna is in her early 30s and she is unmarried with no children. She has no prior work experience and came straight from the MBA program in the same department. She is currently taking Internet Security Seminar class with Dr. Bright, where a term paper for the class will be due in December. The term paper is expected to address the risks and threats of computer and internet business processes to universities. She felt that starting the term paper based on the influences of HI early in the semester should give her a great head-start into her final paper.

2. The Associate Director of IT

Gary Press has been the Associate Director of the Office of Information Technology at MSU since November 1993. He is currently 54, got his Bachelor's degree from MSU (class of 1979) in Pre-Medicine with a concentration in Biology and Physics, and has been in the systems engineering and computer networks for over 30 years. Gary has had previous DRP experience in his capacity as a consultant for FEMA (Federal Emergency Management Agency) where he designed and supported network system redundancy for the federal government's emergency management systems protocol. Mr. Press's duties include authoring the existing MSU DRP Plan and serving on the MSU Crisis Management Team.

3. Morgan State University

According to Wikipedia, Morgan State University is located in Baltimore, Maryland and has an academic staff of 437, administrative staff of 1,556, Undergraduates of 6,400, and postgraduates of 1,027. MSU is a public institution, a Historical Black College and University (HBCU) that was founded in 1867, and is located in an urban environment on 143 acres of land. Some of the key business processes of MSU include records of students' registration, students' academic records, students' financial aid records, human resources and payroll of employees, class schedules, students' class enrollment, transcript services, parking services, library records and computer services, MSU assets and revenues, MSU payouts and liabilities, as well as other data that the school depends on for daily business operations.

4. Basis for the Research

When there is a disaster, demand increases for continuous operation of databases or business processes (Molina & Polyzois 1990). Anna reasons that it is necessary for universities to know if they are prepared enough to keep their business processes going regardless of the level of disaster and that it is also paramount to have a disaster recovery plan in order for universities to maintain a level of business credibility to both customers and stakeholders.

Risk management and disaster recovery are closely related and they are done before disaster occurs (Fallara 2003). Anna believes that universities should display their disaster recovery commitment on their corporate website to show that they are universities who are proactive against losing the credibility, integrity, privacy, confidentiality, and availability of their services to their customers and stakeholders.

The main duties of a disaster recovery coordinator are business impact analysis and defining recovery plans (Fallara 2003). Anna concludes that in order to create disaster recovery plan that is effective enough to recover from any disaster, prevent it, minimize it, or detect it; a university must be able to plan for each of the subsets of both business impact analysis as well as recovery plans.

5. Risk Management Techniques

In order to protect a business from disaster, all threats, vulnerabilities, critical business processes, and components of a business must be identified by recovery planner (Fallara 2003). "The four major steps that are key to planning for disaster recovery or risk management are identifying business process associated with IT infrastructure, prioritizing the business processes according to time sensitivity as well as criticality, identifying existing threats to business processes and infrastructure resources, and defining strategies to eliminate risk and minimize the impact of the risk that cannot be avoided" (Fallara 2003). To have a good understanding of a business process, employees must be used to collect data about the business. Employees are the best informants because they provide information in a detailed format (Fallara 2003).

Gary says, "MSU collects data such as student records, financial records, as well as personnel records, and is stored in a BANNER database. The database is updated daily with inputs from various departments and they are stored immediately. Each department and their employees are responsible in making sure that their records in the database is up-to-date and is effectively and efficiently stored."

When determining what is critical to a business process, which means what is necessary to keep the business alive, you must measure tolerance and criticality. "Tolerance is the ability for a business to cope with disaster interruption while criticality is cost entailed for the business process to be out temporarily" (Fallara 2003).

5.1. Tolerance Levels and Criticality

Table 1: MSU's Table of Tolerance Levels and Their Criticality

Levels	Tolerance	Criticality
1	It is the least impact. It includes single user hardware and software failure, single building hardware connectivity failure, single computer file is unavailable for normal use, members of a critical operation staff are absent, and a single disk crash or failure.	Brought to normal operations within hours
2	It leads to moderate critical impact to MSU's normal operational needs. It includes unavailability of multiple computer files servers, Alpha server is down, service to multiple buildings are down, segment of the campus gigabit backbone is down, internet is down, multiple disk crash, system and user data is lost or corrupted, multiple campus building are without connectivity, and the entire campus is unable to get network printing services.	Brought to normal operations within hours or a few days
3	It is regarded as a minor catastrophe impact. It includes unavailability of main computer facilities for a few days, some systems are unavailable for use, major portion of the production disk is corrupted, unavailability of facility resources for some days, campus gigabit backbone is damaged beyond short term repair, unavailability of entire campus phone system for days.	Brought to normal operations within days or within a week
4	It is regarded as a major catastrophe and resources are unavailable for an extended period. It deals with catastrophes or a natural disaster (tsunami, fire, earthquake etc) that lead to the unavailability of the central computer facilities, most hardware destroyed, total destruction of major production system software, and the entire campus phone system is down for a long while.	Brought to normal operations within weeks or months

Gary adds, "MSU has a current IT Disaster recovery plan that had four emergency tolerance levels which have specific characteristics and procedures to mitigate the particular problem situations."

5.2. Outage Time and Down Time

Cost, security, outage time, and integration are factors that must be considered when planning recovery strategies to restore IT operations quickly and effectively in the case of a service disruption (Fallara 2003). "To determine the impact a process has if it is out temporarily is the outage time. Outage time can be measured as the maximum amount of time a process does not have to work to affect the performance of the system and while the down time measures how the outage time affect other business resources and processes" (Fallara 2003).

Gary states, "In MSU, the duration of outrage time depends on the level of tolerance of emergency. In lower level emergencies, there is enough system redundancy built into the design so that end users will not even know that there is a problem. For instance, there is Redundant Array of Independent Disk (RAID) and hot-swap capability to replace the disk immediately. The configuration in the RAID could be mirroring or striping. Mirroring is two disks storing information at the same time, but only one is utilized. So when one is affected during service, the second can take over without the users knowing. Striping means that both disks store and serve at the same time, so if one fails, the other keeps going."

Savage & Wilkes (1996) suggest a better form of RAID called the A Frequently Redundant Array of Independent Disks (AFRAID). They suggested that AFRAID was designed to make sure that stored data is always available despite disk failure at a significantly reduced cost in performance and eliminate the plagues of traditional 5 disk arrays. AFRAID allows enhances performance and availability by applying data updates instantly and delaying equivalent data updates to the next quiet period between client activity (Savage & Wilkes, 1996). AFRAID has the potential of less data loss and selecting quantity and quality of availability in particular situations (Savage & Wilkes 1996).

Gary instructs, "When there is malfunction with network components in each building, there is certain amount of redundancy of power supply, modules etc, so that users are unaware of any issues. Dual power supplies are used to power the disk cabinets in case the primary power source fails. The disk arrays too have cache battery modules that provide local power source."

Raynham & Tuttle (1998) patented and suggested a low cost and low complexity of redundant power for electronic systems, which reduces system failure rate and enhances system availability. This system is made up of a server and storage system devices. While the storage system has the redundant power supply to overcome power failure, the server power is the source of power for the storage system (Raynham & Tuttle 1998).

Gary emphasizes, "When it comes to common network components that affect a department or a building floor, there are limited spares to make replacements before replacements are shipped overnight. For severe emergency situations, MSU can move to a different campus location (or leased trailers). The outage may last for a week or two depending on how fast the facilities are prepared. MSU contingency agreement with Hewlett Packard (HP) that require that all replacement systems are built or reconfigured within 72 hours, after which MSU staff have approximately 2 days to verify and restore data from backup tapes. Most, if not all, MSU business processes are dependent on the central data systems, so until the system and data are restored, only a few, if any, of the business processes can be in operation."

6. Computer Security

A threat is a set of circumstances that can cost harm or loss to a business. According to the NIST handbook, a format of identifying threats is by grouping them in three parts, which are threat sources, threat motivation, and threat action. The three security requirements of computer security are confidentiality, integrity, and availability and some of the threat prevention techniques are encryption, intrusion detection systems, and firewalls (Fallara 2003).

Gary says, "Disaster recovery deals more with data availability which is part of our recovery plans. For the issues of confidentiality and integrity, all the critical data for the university processes is stored daily to tapes that are encrypted. These tapes are stored on campus in a building different from where the system is located as well as off campus in locked facilities."

Table 2: Table of Security Techniques, Data Availability, Security Controls and Functions

Security Techniques	**Data Availability**	**Security Controls**	**Security Function**
Firewalls	Typical	Preventive	Prevent computers from receiving and sending data that does not meet the set security expectations
Antivirus	Typical	Preventive	Scans computer systems to identify, fix, and remove unwanted software
Intrusion Detection	Typical	Detective	Detects intruders before they enter the system or as soon as they enter
Logging	Possible	Detective	Records activities to know when a problem occurred
Recovery	Typical	Corrective	Brings a system back to normal operation after an attack threat

According to Hua, Patel, & Zaveri (2009), firewalls, antivirus, recovery, and intrusion detection are very typical information system security requirements for data availability, while cryptography and logging were possible. Cramer, Cannady, & Harrell (1996) state that "an effective intrusion detection system should have timeliness, high probability detection, low false-alarm rate, specificity, scalability, and low a priori information". The authors explain that timeliness is detecting intrusion as soon as possible, high probability detection is recognizing all or most intrusion by being up-to-date, low false alarm rate is given credible alarm for real threats, specificity is giving clear description of attack to generate the exact response, scalability is being applicable to various networks, and low a priori information is having the least required information about the potential attackers and their methods.

7. Recovery Strategies

Recovery plans requires a back up strategy, where data and records are stored offsite (Fallara 2003). During the recovery of the primary database, the backup should be able to provide all the changes that took place during the outage of the primary database (Molina & Polyzois 1990). Back up should be able to assist with business transactions when database entry and software are updating in the primary database (Molina & Polyzois 1990).

Alternate sites can be cold, warm, mobile, mirrored, and hot (Fallara 2003). According to Fallara (2003), cold sites basically have electricity, telecommunications, and environmental control; warm sites have equipment, hardware, and software added; mobile sites are warm sites that are mobile; hot sites have support personnel included; and mirrored sites are fully staffed and ready with real time information. From the above information, it is unwise and a resource waste to have a cold and hot sites. It is better to invest in one or upgrade to the next level.

Table 3: Difference between Alternate Sites & their Requirements

Cold Site	**Warm Site**	**Mobile Site**	**Hot Site**	**Mirrored Site**
Electricity Telecom Controls	Cold Site + Equipment HW / SW	Warm Site + Mobility	Warm Site + Personnel	Hot Site + Fully staffed Real time data

Recovery periods usually come with the opportunity to strengthen organizational capacity in localities that had a disaster in order to enhance their economic, social, and physical development (Berke, Kartez, & Wenger 1993).

Gary explains, “The off-site storage facilities for backup data storage are located a quarter mile from MSU and the backup is stored there daily. MSU has no hot sites yet, but there are reciprocal contingency agreements in place to utilize space at Coppin State University in Baltimore as well as Estuarine Center in eastern Maryland. The State of Maryland is talking about constructing a Disaster Recovery Off-Site facility that could be shared by groups of state agencies, which includes MSU, to house racks and hot systems that can be deployed in very short order.”

Anna asks, “What would then happen to our online classes if there was an earthquake right now?”

Gary responds, “An existing contract with Cisco would provide replacement components that will be installed and deployed at the cold site to provide the required emergency internet services. The course content will be restored by each academic department. If most of MSU have been damaged, there is a hierarchical star-switch router network deployed around campus that redeploys fiber through the air-blown fiber system (ABF) if the hard-wire cable is unavailable.”

7.1. Equipment Replacement Plan

“Equipment replacement is making equipment (hardware and software) available through vendor contracts, equipment inventory, and existing compatible equipments” (Fallara 2003).

Gary comments, "Aside from the service level agreement (SLA) that requires HP to replace and reconfigure a designated list of critical equipments within 72 hours after a problem has being diagnosed, MSU also has a network component covered by a SmartNet Maintenance Agreement with Cisco to provide overnight shipment of equipment replacement. MSU is also negotiating a value at risk (VAR) with Cisco to provide extended on-site services to restore the network components and configuration in the case of a major catastrophe. For normal equipment replacements, upgrades, and enhancement, they are done on an as need basis depending on funds and process requirements."

Employees with access are the biggest threat to a security system and they are responsible for majority of the security attacks on a corporate computer system or network (US Department of Energy, Sadowsky *et al.* 2003, Igure & Williams 2006, Patel *et al.* 2008, Patel & Zaveri 2010, Ventuneac *et al.* 2003, Byres & Hoffman 2003).

Anna asks, "What if the employee in charge of the (SAN) disk and back-up tape copies decided to destroy them or corrupt the data integrity?"

Gary answers, "In the case of an employee purposely and physically damaging the storage area network (SAN) disk, the two back-up tape copies, as well as compromising the data integrity, MSU has not considered this reality yet. MSU will plan to have two employees, instead of just one long time trusted employee, store each of the back-up tape copies."

8. Recovery Plans

Employees should make up the support teams and they are to be assigned to particular equipment and functions (Fallara 2003). MSU has different employees manage various functions at different tolerance levels.

Anna adds, "All these disaster recovery team functions will be meaningless if the business process data that is being recovered from a disaster to prevent the continuous interruption of the business process is inaccurate, incomplete, inconsistent, and not current before the disaster took place. So the first line of defense against a disaster is an effective and efficient data entry and storage before the disaster occurs. "

Scannapieco, Missier, & Batini (2005) state that for any data to have quality and value; it must be accurate, complete, current, and consistent. Accuracy means all letters, numbers, or symbols are in the right place and are free from error. Complete means all necessary fields for a subject (student, faculty, staff, or building) are filled totally. Current means that the information is up-to-date (age, address, status, position, or class). Consistent means all the data of a subject matches (age must match birthday and gender must match subject).

Table 4: Table of Recovery Support Team Members & their Functions

Levels	Support Team Members	Function
1	Director and Associate Director of Office of Information Technology (OIT)	Coordinates the recovery services
	Director of Technical Support	Manages hardware and software repairs and replacements
	Supervisor of Program Services	Coordinates software recovery and reconfiguration
	Associate Director of OIT	Manage administrative cluster system's repair and recovery
	Senior Network Analyst	Restores computer systems, servers, network communications, and internet services
2	Director of OIT	Chairs the committee and is assisted by the Physical Plant Department (PPD)
	Associate Director of OIT	Coordinates all production system hardware and operating systems
	Senior Network Analyst	Rebuilds computer file servers and recover information from backup tapes for system restoration to original state
	University Topologist	Coordinates all data infrastructure requirements
	Supervisor of Administrative Computing Operation	Provides computer room operators the data to restore system to its latest and validate the integrity of the databases
3	Network Topologist	Works on the infrastructure, video systems and fiber re-development
	Manager Voice System Technical Support	Works on voice systems and cabling infrastructure
	Associate Director of OIT	Administers recovery of computing systems
	Supervisor of Programming	Administers recovery of computing software application
	Supervisory Administrative Data Operations	Works on restoration of data
	Senior Analyst	Works on administrative network systems, server recovery, and WAN services
	Academic Systems Manager	Works on recovery of academic computing systems
	Senior Technical Support Analyst	Works on recovery of Application server
4	Director of OIT	Chairs Disaster Recovery Planning committee, assesses damage, and coordinate IT systems and software recovery
	Physical Plan Director	Coordinates the feasibility of using alternate facilities based on the committee's plan for the recovery and relocation efforts
	Director of Procurement and Property Control	Works to get the funding and rental contracts required for temporary relocation
	Associate Director of OIT	Works with vendor (HP) to assess salvageable resources and assist vendor in timely replacement and successful reconfiguration of hardware and software in order to return the system to a functional state at alternate site
	Director of Technical Support, Topologist, and Manager of Voice Communication Technical Support	Accesses damage to cabling infrastructure, WAN systems, phone system, and videos are recovered properly at the alternate site
	Supervisor of Programming, Lead Programming Financial Systems, and Lead Programming for Human Resources Systems	Accesses damage to software applications and restore production systems to operational status after hardware is restored
	Supervisor of Data Operation	Provides data operator support to restore data from tapes backup to return the cluster operating system and the online application to a pre-disaster state

8.1. Training and Maintenance

"Training and maintenance should include both classroom exercises, where employees are walked through procedures and functional exercise is a hand-on disaster scenario that should not affect normal operations" (Fallara 2003). MSU has IT Disaster Test Plan that should be practiced once a year. It has specific exercises that staff will practice based on various stimulated emergency scenarios.

9. Anna's Disaster Recovery Score

Simpson (2008) in Table 5 shows that the formula for calculating disaster preparedness (DP) measure or score for a city is:

PM = 3(A + B + C) + 2(D) + 3 (E) + 3(F) + G + (-) H + 3(I) + J.

Each letter represents a disaster preparedness factor, whose sub-factors may have data type of a number, yes/no, or are scaled. The number data was calculate with a formula or were actual numbers (radio station = 3), yes/no had a value of one for YES and a value of zero for NO, and the scaled data used actual numbers to multiply set figures (earthquake = MM scale X -10) or where simply assigned a score based on their ratings (AAA = 3). The scores where then added up to give the disaster preparedness measures or score for a city.

Table 5: Table of the Factors of Disaster Preparedness and their Respective Measurement Points

Letter	DP factors	Some sub-factors	Points	Point Justification
A	Fire Protection	# of employees, vehicles, stations	3	Core DP emergency response
B	Emergency Med. Service	# of employees, hospitals	3	Core DP emergency response
C	Public Safety/Police	# of employees, funds	3	Core DP emergency response
D	Planning and Zoning	Pre-exist. ordinance, hazard maps	2	FEMA estimation in DP investment*
E	Emergency Mgmt. Office	Emergency plan, training, funds	3	Core DP emergency response
F	Other Emergency Func.	Mass care sites, recovery groups	3	Core DP emergency response
G	Add. Comm. Measures	Social services, volunteer	1	Neutral
H	Hazard Exposure	Nuclear, earthquake, chemical	-1	Higher risk
I	Evacuation & Warnings	Evacuation plan, warning systems	3	Core DP emergency response
J	Community Resiliency	Cash, city budget	1	Neutral

Anna decided to create her own disaster recovery preparedness score (DRPS) for universities based on the table form (Simpson 2008) and Gary's response for MSU. She felt that computer security should be given 1 point because data integrity and confidentiality were expected to be mandatory for any university's computer system. Collection of business process data was given 2 points and the frequency was given a point. Full points will be awarded to efficient electronic data collection with immediate data storage in the database, which should be updated regularly within each day. The tolerance levels should be given 2 points and their critical levels get a point. This shows that they have a plan.

Having an alternate recovery site gets two points, but that alternate site should be located far away from the university in order to avoid the disaster that affects the university. This gets a point. The equipment gets two points while its replacement plan gets a point. DR support team members must have efficient assigned roles to get 3 points, while multiple employees should have access to backup disks and tapes to get a point. Effective DR training and maintenance get two points, while its frequency for staff development gets a point.

Table 6: Table of the Factors of Disaster Recovery Preparedness and their Respective Measurement Points

Letter	Disaster Recovery Preparedness & Points	Total Points
A	Computer Security: Confidentiality & integrity (1)	1
B	Collect business process data (2); Data stored immediately (1)	3
C	Adequate tolerance levels (2); Efficient critical measures (1)	3
D	Alternative recovery site (2); Adequate location of alternative recovery site (1)	3
E	Adequate equipment plan (2); Efficient equipment replacement plan	3
F	Great DR support team with assigned roles (3); Many employees with backup disks & tapes (1)	4
G	Effective DR training & maintenance (2); Frequency of training and maintenance (1)	3
Grand Total	Disaster Recovery Preparedness Score for Universities	20 (100%)

Anna summarizes, "The DRPS should be based totally on all employee surveys, which should be completed electronically to ensure privacy. Also, the results should be stored in a database and scored with data mining software. In all these factors of DRPS, a zero point should be given when a factor is absent or inadequate, and given full points if the factors are present. Full point is given if employee survey results are greater than 80% approval. The only two exceptions are a university gets a zero out of a point if the alternate site is inadequately located, and the DR support teams gets a point out of three, if all employees are not stated in their support group. This is because the alternate site is useless if the disaster affects it, and data should be documented and entered by all employees accurately as well as stored in a timely manner for data to be of any value in the first place for recovery. The DRPS has a total of 20 points, but should be multiplied by 5 to have a percentage score based on 100. Based on this MSU should be able to survive HI effectively. Hopefully, universities would adopt this score as a way to inform their customers and stakeholders that the business processes and business data are safe and secured to continue operation and survive a major disaster. Government can also encourage universities to place their DRPS on their website to show how credible they are."

4. Epilogue

Two days after HI passed Maryland; Anna contacted Gary to find out how HI affected MSU's business operations. She was concerned because that Saturday, there were lots of sirens and fire trucks going about on the roads around the school's residence. In fact there was loss of power for a few seconds and then it came back. She wondered if there was any destruction to property or service system that disrupted MSU's business processes. Anna emailed Gary for a feedback.

Gary responded that only Saturday classes were cancelled because of the expected severe weather of the approaching storm, but no business processes were affected. He added, "There was no special preparation made for the storm and if power had been lost, the UPS (Uninterrupted Power Supply) backup would have kicked in until the backup generator would have taken over to prevent any transient power loss from affecting the systems."

Gary emphasized, "Routine full backups were performed on Friday night and Saturday morning. We were not really that worried because the storm was not expected to cause severe physical damage. If power had been lost to the facility, the UPS or generator backup systems would have protected the hardware from power outage and spikes."

5. Limitations

More articles could have been used to evaluate MSU disaster recovery preparedness, but these articles were sufficient. Quantitative surveys or questionnaires could have been utilized, but these qualitative questions were preferred in order for the MSU staff to tell us exactly what their disaster recover preparedness was rather than have them grade the quality of it. This method allows us to evaluate MSU's DRP rather than them evaluating themselves.

6. Conclusion

MSU disaster recovery plan is adequate. They had an efficient plan and level of preparedness in place. MSU met the minimum requirement to tackle the various factors effectively and efficiently in case of a disaster. I will recommend that MSU tried to acquire the 5 disk AFRAID system rather than the two disk system they currently have. AFRAID makes sure that stored data is always available despite disk failure; it significantly reduces cost in performance, as well as eliminates the plagues of traditional 5 disk arrays.

The patented low cost and low complexity of redundant power for electronic systems that minimized system failure rate and improves system availability is also recommended for MSU. This system has a server and storage system devices for redundant power supply to act against power failure while the server power acts as a source of power for the storage system.

Lastly, MSU should have two employees, who may not know each other, store the back-up tapes. This will be security at its best because two employees can collaborate to be a very destructive and disruptive force. So if one employee "messes up", we know for sure that quality data can be retrieved from the other employees in real time.

7. Contribution

Having a disaster recovery preparedness plan is very necessary considering the fact that earthquakes, hurricanes, fires, and tsunamis can occur at any time. I believe that there should be federal and states laws implemented to make sure that most universities are prepared for disaster recovery for consumer and stockholder's safety and business interests.

It should also be seen by Government as a defensive strategy of fighting terrorist or cyber invaders who may be interested in attacking the country through our financial, economic, and privacy data. Also, more research needs to be done to come up with a formula for calculating Disaster Recovery Preparedness Score. This score, like a restaurant score, should be placed on corporate websites for potential customers and stakeholders to see before making a business decision about the organization.

The disaster recovery preparedness score should be available on all business and corporate websites as a way to show potential and active customers as well as stakeholders that their business and service with the specific university is secure, credible, guaranteed, and available at any time. This will encourage universities and their employees to see the need for making disaster recovery their individual and business goal by making sure each member of a disaster team knows and takes his or her specific assignment seriously.

References:

Berke, P. R., Kartez, J., & Wenger, D. (1993), "Recovery after disaster: Achieving sustainable development, mitigation, and equity", *Disasters*, 17(2): pp. 93-109.

Byres, E. & Hoffman, D.(2004), "The myths and facts behind cyber security risks and for industrial control systems", VDE Congress, VDE, Berlin, October.

Cramer, M. L., Cannady, J., & Harrell, J. (1996), "New methods of intrusion detection using control-loop measurement", *Technology for Information Systems Security*, 5: pp. 1-10.

Fallara, P. (2003), "Disaster recovery planning". Institute of Electrical and Electronics Engineers (IEEE) Potentials, pp. 42-44.

Hua, J., Patel, S., & Zaveri, J. (2009), "Securing business information systems from cyber-attacks", *Journal of Digital Business*, 3(1-2): pp. 35-53.

Igure, V. M. & Williams, R. D. (2006), "Security and SCADA protocols", *NPIC&HMIT*, pp. 560-567.

Molina, H. & Polyzois, C. A. (1990), "Issues of disaster recovery". Institute of Electrical and Electronics Engineers (IEEE), pp. 573-577.

National Institute of Standards and Technology (1995), "Logical Control Access", *The NIST Handbook*, 800(12): pp.194-212.

Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008), "Quantitatively assessing the vulnerability of critical information stems: A new method for evaluating security enhancements", *International Journal of Information Management*, 28(6): pp. 483-491.

Patel, S. & Zaveri, J. (2010), "A risk assessment model for cyber attacks on information systems", *Journal of Computers*, 5(3): pp. 352-359.

Raynham, M. B. & Tuttle, M. R. (1995), "Redundant power supply and storage system", *United States Patent*, pp. 1-10.

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A. (2003), "Personnel security", *IT Security: Information Technology Security Handbook*, pp. 112-116.

Savage, S. & Wilkes, J. (1996), "AFRAID – A frequently redundant array of independent disks". USENIX 1996 Annual Technical Conference, pp. 1-13.

Scannapieco, M., Missier, P., & Batini, C. (2005), "Data quality at a glance", *Datenbank-Spektrum*, pp. 6-14.

Simpson, D. M. (2008), "Disaster Preparedness Measures: A test case development and application", *Disaster Prevention and Management*, 17(5): pp. 645-661.

US Department of Energy, *21 Steps to Improve Cyber Security of SCADA Network*. Office of Energy Assurance, Office of Independent Oversite and Performance Assurance, pp. 1-8.

Ventuneac, M., Coffey, T., & Salomie, I. (2003), "A policy-based security framework for web-enabled applications". Proceedings of the 1st international symposium on Information and communication technologies, Dublin, Ireland, pp. 487- 492.

Wikipedia, http://en.wikipedia.org/wiki/Morgan_State_University