# Improving Service Continuity: IT Disaster Prevention and Mitigation for Data Centers

Louis Turnbull Henry Ochieng Chris Kadlec Jordan Shropshire

Georgia Southern University
Dept. of Information Technology
P.O. Box 8150
Statesboro, GA 30460
(912)478-4848

louisturnbull@gmail.com ho00027@georgiasouthern.edu cakadlec@gmail.com jshropshire@georgiasouthern.edu

## ABSTRACT
Data centers provide highly-scalable and reliable computing for enterprise services such as web hosting, email, applications, and file storage. Because they integrate a range of different systems, data center administration is a complex process. Managing the risk of IT disaster is especially difficult. Layers of interrelated infrastructure multiply the effect of system malfunctions. Seemingly-small problems can turn into major disasters and take entire data centers offline. To cope with the myriad risks, this research develops a matrix of IT disaster prevention and mitigation techniques for data centers. The matrix is organized along two dimensions: attributes of data center infrastructure and elements of the IT disaster recovery process. It includes 134 specific techniques which were clustered into 49 cells within the matrix. An expert panel assessed the validity of the matrix and ranked the techniques within each cell. The result is a comprehensive tool for improving the resilience of data centers.

## Categories and Subject Descriptors
D.4.5 [**Reliability**]: Backup procedures, Fault-tolerance, Verification.

## Keywords
Data centers, IT disaster recovery, mitigation, infrastructure.

## 1. INTRODUCTION
Data centers are the building blocks of cloud computing systems. They incorporate commodity servers, storage arrays, and high-throughput networks into physical structures to support enterprise computing. In the aggregate, they provide a highly-scalable platform for providing information services such as email, applications, and document storage. Because they integrate a range of different systems, data centers require careful management. Relatively small errors in configuration, minor security flaws, and isolated hardware failures have a significant effect on the stability of information services. They may even bring entire data centers offline. For instance, contractors installing a sprinkler system could accidently cut through major fiber line. Cooling systems, when facing extreme temperature swings, can overcompensate and freeze over. In such cases, they must be shut down in order to thaw. Emergency utility repairs can lead to power surges and trip power circuits or create brownouts. Unknowing employees may introduce worms and viruses into trusted zones by using infected thumb drives. Distributed denial-of-service attacks overwhelm networks and servers, blocking legitimate users from accessing services. Because relatively minor events can cause major catastrophes, IT disaster recovery planning is essential. Although it is not possible to predict every possible disaster scenario, data centers should account for a wide range of contingencies.

To assist in the planning process, a matrix of IT disaster recovery techniques was developed. It contains a comprehensive listing of disaster prevention and mitigation techniques specifically for data centers. The matrix is organized along two axes: data center infrastructure attributes and elements of the IT disaster recovery process. Prior research indicated that the infrastructure attributes of the data center should be organized into the following seven attributes: service, application, operating system, computer hardware, networking, utilities, and the physical structure layer. The IT disaster recovery and mitigation is structured into seven elements: IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance procedures.

To populate the matrix, a team of graduate researchers performed an extensive review of over 150 articles. Using the content analysis method, 134 disaster prevention and mitigation techniques were extracted. The techniques were clustered into the most appropriate cells inside the matrix. The resulting framework was refined over multiple iterations. To assess content validity, the matrix was reviewed by a panel of IT researchers who specialize in IT data center management. The panel assessed the completeness of the matrix and ranked the techniques within each cell. The results can be used to improve IT disaster preparedness. This manuscript is organized as follows: first background information on data centers and IT disaster recovery is presented. Next, the research methodology is described and the resulting


*RIIT'13,* October 10–12, 2013, Orlando, Florida, USA.

http://dx.doi.org/10.1145/2512209.2512213

matrix is introduced, followed by the results, implications and conclusions.

# 2. BACKGROUND

## 2.1 Data Centers

As cloud computing increases, so does our dependence on data centers for information service provisioning. Data centers are facilities that house high-performance computers, storage servers, computer servers, networking or other information technology (IT) equipment. They are the building blocks for cloud computing systems. They perform essential duties such as hosting, meta-scale processing, and storage. These data centers host servers and applications that clients use to operate their business [1]. Data centers either support internal clients or act as infrastructure providers (i.e. Google, Microsoft, and Amazon) for external clients. To increase economies of scale and ensure uptime, infrastructure as a service (IaaS) providers are rapidly building geographically-distributed cloud data centers. They support a variety of cloud-based services such as email, web servers, storage, search and instant messaging [2].

## 2.2 IT Disaster Recovery

Due to its importance in averting disasters and ensuring the continuity of organizations, the concept of IT disaster recovery planning is acquiring an increased amount of attention from IT practitioners and business managers [3]. A disaster recovery plan is a blueprint for recovering from such events and is intended to increase chances of survival and reducing the risk of loss [4]. The purpose of an IT disaster recovery plan is not to simplify IT services that eases restoration, but devise alternative ways of restoring IT services so that service can be brought back online and be sustainable following disaster. IT disaster recovery can be defined as set of actions that an organization follows to improve its ability to resume its IT services after a disaster.

# 3. CONCEPTUAL DEVELOPMENT

This research develops a matrix of strategies for helping data centers cope with the risk of IT disasters. A comprehensive listing of specific tools and techniques was drawn from contemporary articles from industry and academia. The resulting elicitation was organized along two dimensions – components of data centers (See table 1) and elements of the disaster recovery process (See table 2). For instance, a specific technique might be found to impact one component of a data center, and assist in one step in the IT disaster recovery process. These dimensions were based on constructs which were broken into categories in previous studies. By organizing along these dimensions, it is possible for IT professionals to associate a specific cell with a weakness and locate the best solution. Because the cells are rank-ordered by a team of respected data center professionals, it is easier to identify the best solution out of multiple options.

# 4. METHODS

Matrix development followed a structured approach in order to increase rigor and build validity. First, a team of graduate student researchers from engineering and information technology performed a comprehensive search of articles relating to disaster recovery for data centers. Using coordinated search terms, over 200 articles were extracted from academic databases and industry outlets. Of these, 114 articles were found to be relevant enough to include in the analysis. These articles were used in a content analysis. The purpose of this analysis was to identify and code IT disaster recovery technique and tools. A previously established coding scheme was used for classifying points [3]. It was developed specifically for IT disaster recovery planning involving infrastructure. Each article was reviewed and useful techniques were coded according to two factors: (1) which data center infrastructure layer they impacted and (2) which part of IT disaster recovery they supported. To provide overlap, each articlewas reviewed by at least two researchers. For cases in which there was disagreement over coding, a third researcher broke the tie. Once all the coded units were collected, they were organized into the matrix. The matrix itself was then refined over three

**Table 1. IT Disaster Recovery Planning**

| Element | Description |
|---|---|
| IT Disaster Identification and Notification | IT disaster identification and notification is an element that focuses on processes that have been founded towards the recognition of IT disasters, communication through times of crisis, and advising designated team members and stakeholders. An array of potential disaster scenarios that may arise include both manmade and natural disasters. |
| Preparing Organizational Members | Preparation of organizational members involves developing a team dedicated towards IT disaster recovery and mitigation, conferring and strategizing with noteworthy non-members, and constructing a priority-based decision structure catered towards the protection of critical assets. |
| IT Services Analysis | The IT services analysis element is directed towards classifying IT services along with assigning a priority for reactivation, as well as detecting probable threats. IT services should be organized within a scope of reason as to what services are crucial to maintain business continuity and how to identify and neutralize potential risks that will hinder it. |
| Recovery Process | The recovery process pertains to any sort of procedure that will aid in restoring the data center to a suitable and operable state. Recovery involves establishing tactics with the goal of minimizing downtime and reinstating business continuity in an expedient manner. |
| Backup Procedures | Backup procedures are adequately designed preparations or blueprints utilized to provide a viable replication of a data center constituent. |
| Offsite Storage | The element of offsite storage relates the separation and securement of data or resources from the data center facility. This spans from utilizing cloud infrastructure, to consuming warehouse space, relocating resources, and even to instituting an alternative data center. |
| Maintenance | Maintenance with regards to the data center incorporates testing and sustaining the functionality of resources, documenting the configuration of hardware and software, assessing the disaster recovery plan, and synchronizing the recovery plan with business continuity. |

**Table 2. Data Center Layers**

| Attribute | Description |
|---|---|
| Physical Structure | The physical structure layer for a data center consists of a building or a structure within the same geographic plane. It will also include racks for the hardware, track systems for cables, wiring, building access control systems, and power management systems. |
| Utilities | The utilities layer consists of a multitude of data center resource systems. These systems include heating, ventilation, air conditioning, power distribution, water supply, fuel reservoirs, waste disposal, fire suppression systems (FM-200), and communications (telecom and internet service provision). The utilities layer also includes standby systems such as power generators, reserve batteries, uninterruptable power supplies, portable chillers, and alternative energy sources. |
| Networking | The networking layer pertains to all hardware and software that is utilized in a fully functional network. This layer consists of cabling, routers, switches, wireless connection points, virtual and physical firewalls, security protocols, administration, data management, and connectivity access. |
| Computer Hardware | The computer hardware layer incorporates server systems, hypervisors, storage devices (hard disks, USB drives, compact disks, data tapes), workstations, personal computing components (memory modules, central processing units, and mother boards), as well as sensor systems. |
| Operating System | The operating system layer consists of any operating system (OS) that functions on any piece of equipment. This would incorporate a server system OS, workstation OS, smart phone OS, and especially virtualization OS (for the hypervisor and virtual machines). |
| Application | The application layer contains software, data, algorithms, configurable settings, downloadable updates, digital documents, executable files, scripts, hardware firmware, and anything else that involves consolidated hosting. |
| Service | The service layer is a compilation of examination and load stabilizing tools for data centers to deliver services. This may also include pertinent services such as email, web hosting, third party services for data backup and recovery, and provisioning services in virtualization (hardware, software, and infrastructure-as-a-service). |

iterations. For each iteration, the researchers sought to identify redundancies, under-represented topics, and content which was not an integral part of disaster recovery. After three rounds of revision, the result was a matrix consisting of 49 cells and 134 recommendations for coping with the risk of IT disaster. This matrix was then distributed to an expert panel comprised of 5 IT professionals with expertise in disaster recovery and/or data center management. The panel was given two tasks: assess the completeness of the matrix and rank-order the contents in each cell. Following two rounds of feedback and revision, the panel confirmed the content validity of the matrix and agreed to the ranking of disaster recovery techniques within each cell.

# 5. RESULTS

A collection of 134 notable recommendations were derived from the research. The results were organized into a two dimensional matrix. The row header is formed as the dimensional elements of IT disaster recovery, Table 1. The column header is formed as the attribute layers of the data center, Table 2. When brought together, an easily decipherable matrix helps IT professionals pinpoint to the appropriate disaster mitigation and recovery reference as needed. A blank matrix template can be used as a starting point for data center managers to evaluate their own disaster recovery solutions and build upon areas of identified weakness. This also aids in laying the foundation for a solid plan to present for funding resources in protecting the data center. The following matrix is an organized subsystem of the extracted recommendations. Each subsystem forms an order of priority starting with the physical structure attribute through to the service attribute. This is based on the fact that if there is the elimination of a prior attribute, the proceeding attributes will cease to exist. Incorporated amongst the attribute subsections are comprised of a mixture of the recommendations that are characterized towards the elements of IT disaster recovery. In order to understand how the disaster mitigation and recovery process is achieved, it is necessary to comprehend the criterion of the dimensional elements of recovery first. Afterwards the mitigation and recovery techniques can then be processed and applied as needed.

The data center has been broken down into logical sections, according to the developed matrix, and addressed with disaster mitigation and recovery. A summary of the collected techniques is presented as such.

## 5.1 Physical Structure

First, there is the physical structure of the data center which houses and protects the core of the business. Therefore, the protection and maintenance of the structure is important. Initiate this by monitoring local meteorological forecasts and news media regularly for potential threats (weather, terrorism, etc.). Assign threat levels to disaster scenarios and create an occupancy evacuation plan. Designate specific emergency action responsibilities to selected members of the organization. Train all of the staff regularly as preparation for potential disasters. The training should take place in the form of conducting building exit strategies, ensuring that the physical structure is secure from further damage, containment of disasters, and establishing emergency protocols. Lastly, be restrictive with building access. Monitor all entry and exit points of the structure. The ultimate protection is having alternate facilities themselves.

## 5.2 Utilities

Utilities are an essential part of every data center and allow the operability of resources to exist. To start, secure the HVAC system to recirculate air to avoid the intake and dispersion of particulate matter. Monitor the utilities by installing sensors to alert staff of humidity levels, unsafe temperatures, and unauthorized access. Establish teams to recover utilities assuring there are personnel overlaps and redundancies. Update and post utility provider contact information (of all utilities) and prepare staff members on how to report a utility failure or obtain status updates on repairs. Since most key utilities cannot be moved, such as water lines and power lines, establish alternate routes for utilities to service the data center. Maintain adequate fuel supplies

for generators and refill fire suppression systems. Review and test backup procedures at the utilities layer on a regular basis.

## 5.3 Networking

Networking inside the data center consists of a line of interconnectivity between critical hardware components. In order to protect the network assets, identify all networking systems running in the data center and establish priorities of reactivation. Install application level firewalls along with other intrusion prevention systems. This will help identify initial threats within the networking attribute. Also, monitor the behavior of users and hosts by observing for abnormalities. Organize and establish teams to recover networking systems by assuring there are personnel overlaps and redundancies. Once teams have been arranged, backup network configurations and network maps. Consider establishing procedures to recover networking or move the networking to alternative locations. Secure additional hardware equipment (servers, routers, switches) and software licenses to enable the continuity of the data center network operations. Consider virtualization or cloud computing as a method of offsite networking. Finally, review and test backup procedures at the networking layer on a regular basis.

## 5.4 Computer Hardware

Start by analyzing all of the computer hardware that is present in the data center and address service contracts with vendors regarding the equipment for replacement and repair issues. Provide at least one set of comparable computer hardware to utilize as a replacement in the event of a failure. This could be done through purchasing hot spares or keeping recently retired equipment. Keep backups of physical equipment along with all other backups for the computer hardware at an offsite location. Consider using cloud services as a tool for backing up computer hardware files and configurations. Ensure the cloud system has the sufficient capacity to support the workload of the enterprise.

## 5.5 Operating System

A data center will house a variety of operating systems on a multitude of computing hardware. Software firewalls should be installed to prevent attacks from taking place against all of the operating systems. Identify all operating systems running in the data center and establish priorities of reactivation, along with the potential risk factors that may arise. Create procedures to recover the array of operating systems within the data center. Assemble a select set of team members to execute and refine the recovery procedures. This will expedite in the recovery of the operating systems and help minimize downtime. Include the selection of alternative environments for operating systems to be executed (either physical or virtual) in the event of a disaster. Consider using virtualization technology since OS templates can be imaged within virtual machines for quick deployment. The virtual machines can even undergo live migration across the infrastructure platforms.

## 5.6 Application

The application attribute deals with data, executable files, and pertinent configuration files. In order to protect against disaster,start with installing application level firewalls to prevent attacks on applications. Identify all of the applications running in the data center. Establish procedures to recover applications, and include the relocation of the applications to an alternative platform for execution. Institute training events and educate the employees on the appropriate backup procedures for the applications. Ascertain a priority of how items should be recovered in sequence (proprietary software, sensitive or classified documents, expensive or meaningful scientific data). Develop backup copies of configurations at the application attribute and store them in a safe location.

## 5.7 Service

In order to help mitigate disaster within the service attribute, a disaster response team should be assembled and an appropriate disaster plan must be created. The plan needs to include identifying all of the services offered and establish priorities of reactivation. Establish procedures to recover services or shift services to alternative locations. Devote key staff members to be on call to assist in disaster recovery efforts. Select alternative locations and sources of services to be utilized in the event of a disaster. Training events should be developed and geared towards the inclusion of all of the layers for the data center. Reinforce interface protocols at all levels during training exercises. Review and test backup procedures at the services layer on a regular basis. Finally, establish service level agreements (SLA) for the services provided and monitor these services.

# 6. Conclusions

Safeguarding data centers is no simple task. Inter-reliant systems and the sheer quantity of hardware and software make administration a complex process. Under such conditions, small problems very quickly escalate into major crises. If affected information services are to be restored, then planning is essential. To assist in this process, this research developed a matrix of techniques for preventing and mitigating IT disasters. The matrix was framed along two dimensions – components of data center and elements of IT disaster recovery. The attributes that compile the matrix are structured in order of reliance on each prior element. This starts with the physical attribute representing the most critical aspect of the data center through to the service layer which would not exist without the prior attributes having formed the foundation. Many specific techniques were identified and organized into the framework. The elements in each cell were ranked by a group IT professionals with expertise in data center management in order to prioritize acquisitions. The matrix can be used as a guide to ensure the adequacy of in-place procedures and guide further development. It is expected that the matrix will be refined in future research.

# 7. REFERENCES


[1] Stryer, P., *Understanding Data Centers and Cloud Computing.* Global Knowledge Instructor, 2010.

[2] Benson, T., A. Akella, and D.A. Maltz. *Network traffic characteristics of data centers in the wild*. in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. 2010. ACM.

[3] Shropshire, J. and C. Kadlec, *Developing the IT Disaster Recovery Planning Construct.* Journal of Information Technology Management, 2009. **20**(4): p. 37.

[4] Hiatt, C.J., *A primer for disaster recovery planning in an IT environment*2000: Igi Global.