Disaster Recovery Plan

Author’s name

[Institutional Affiliation(s)]

Author Note

Disaster Recovery Plan

# Overview of Company

IBM is a data consulting corporation head-quartered in New York USA. It is the biggest technology-based company in the world and is the second most valuable IT brand in the world. IBM designs, develops and sells hardware and software solutions and offers, infrastructure services, hosting services and consultancy services in technology ranging from data science to nano-technology. IBM’s corporate mission statement states that,

“To lead in the creation, development and manufacture of the industry’s most advanced information technologies, including computer systems, software, networking systems, storage devices and microelectronics. And our worldwide network of IBM solutions and services professionals translates these advanced technologies into business value for our customers. We translate these advanced technologies into value for our customers through our professional solutions, services and consulting businesses worldwide.”(MSA, 2019)

Through its mission statement, IBM ensures that the company makes its aim of becoming the leader in global market of information technology very clear. The main idea that differentiates IBM from its counterparts is its trust in the leadership abilities of resources from different developing nations. This makes the products introduced by IBM deliver in foreign communities as well as the developer are more considerate of the religious and cultural sensibilities in the region. There is another aspect in which IBM leads the world and that is its leadership ability, it affects and invests in fields and companies that are not directly related to it. This not only increases the influence of the company but also provides its employees necessary exposure so that if need be, that in the future, they introduce themselves in that specific field then they will have some employees with hands-on experience in that field.

Similarly, the vision statement of IBM states that,

“To be the world’s most successful and important information technology company. Successful in helping out customers apply technology to solve their problems. Successful in introducing this extraordinary technology to new customers. Important, because we will continue to be the basic resource of much of what is invested in this industry.”(Lombardo, 2017)

The vision statement of IBM represents its progress path as the corporate continues to maintain its position as one of the best players in the global IT market. The company, like any country emphasizes the development of its brand and its business globally. The vision statement also aspires to help the customers to solve their problem with the use of technology. It also aims to provide new, innovative and extraordinary technology to customers. Apart from this, the thing that can be determined for the vision statement is the idea that the company wants to be the basic resource of much of the investment that the industry receives.

In terms of size, IBM employs a total of 366 thousand employees globally. In terms of its organizational structure, the company has a product-type divisional organizational structure. The divisional organizational structure aims to decrease the company overhead by employing people around geographical, market or product and service groups. Thus, a company like IBM could be organized on divisional lines that could have operating groups based on geographical and production needs. The main characteristic that IBM’s organizational structure has, is the fact that the representation of the business processes involved in the conception, design, development and sale of a product is clear in nature. For example, there can be working divisions based on products that provide a primary structure to the company. The company’s organizational structure supports the use of tactics and techniques that pave the way for the design and development of competitive products.

# Network Architecture

The network architecture that IBM uses is known as systems network architecture. The systems network architecture (SNA) is a network architecture used for data communications developed by IBM to determine the common conventions that will be used for communication in the wide range of IBM communication products and other platforms in the company that are based in both software as well as hardware. In the early years of the company, these protocols were developed and deployed. They ere maintained and developed by IBM for a couple of decades. A lot of other companies used the same conventions and it became a type of networking standard for its time. However, with the development in networking being a continuous process, this networking architecture became obsolete with the passage of time. New networking protocols were developed which were more robust and which are being used to this day, but the time is still far away when all devices using the SNA disappear.

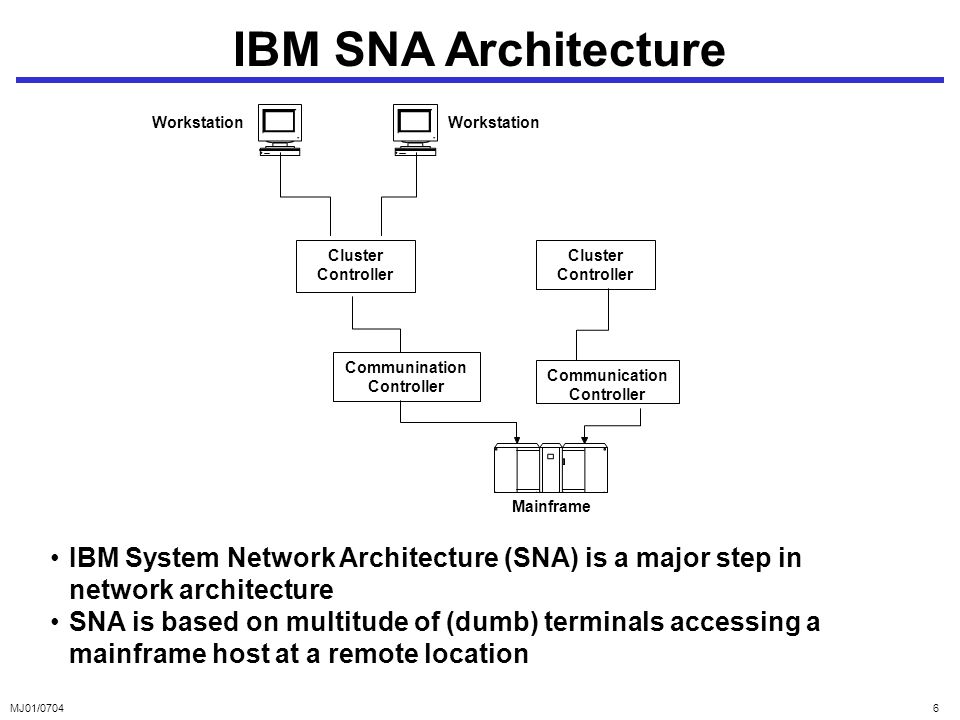
[](https://www.google.com/search?q=systems+network+architecture&tbm=isch&source=iu&ictx=1&fir=xXUba6YyXqcniM%253A%252C8at0k5HqqNe9BM%252C_&vet=1&usg=AI4_-kQFAYSZenpDHXe_vmmYdewEmVTmbQ&sa=X&ved=2ahUKEwi6lvHOtq_mAhX0BGMBHd8NDPQQ9QEwAHoECAgQAw#imgrc=xXUba6YyXqcniM:)

Figure -IBM SNA architecture

# Disaster Recovery Policy

Disaster recovery policy, in essence, is a policy based on a set of protocols, rules and procedure that will be implemented and adopted in the scenario of a disaster. The DRP explains in detail, the roles and responsibilities that will be given to certain individuals that are named as the Incident Response team which would only act in cases of emergency. The types of disasters and the responses are all clearly defined. The way that the company will recover form the incident after the disaster is also explained in great detail in the disaster recovery policy.

## Disaster Declaration

In case of a disaster, the head of the incident response team will assess the situation and declare the disaster in terms of its types and severity. There will be two acronyms used for the declaration of the disaster. The first one will determine the type of disaster while the second one will represent its severity.

1. The first term will clarify whether the nature of the disaster. The acronym used for natural disasters is ND while the one used for cyber disasters is CD.
2. Severity will be determined by the use of a number from 1 to 10 with 1 being the mildest while 10 being the most fatal.

So, the head of the incident response team will declare the disaster as ND6, and the people will get to know that there is a natural disaster with a severity of 6. A severity of a natural disaster above five will automatically trigger the evacuation procedure.

## Assessment of Security

The head of the incident response team along with 3 of its top members are then given the responsibility of security assessment. The security assessment has the following aspects.

The type of disaster answers the question of the type of security assessment that needs to be undertaken.

1. In case of a natural disaster, the area that is most affected will be recognized and all recovery procedures will be directed towards it.
2. In case of a blockade in communication and service, the assessment will include the security analysis of the areas of the facility that are the most affected and that need the most attention.
3. In case of spoofing, the assessment will include prioritizing the channels that are used for outward communication and those channels will be encrypted if necessary.
4. In case of a worm attack, the part of the facility where the data is stored will be temporarily isolated and the worm will be located by the cyber-security professionals and addressed immediately.

## Potential disaster scenarios and action

The following disaster scenarios will be discussed and necessary action will be taken.

1. In case of fire, the company will try to limit the area which is being affected by evacuating the affected building and immediately calling the fire brigade. The company will also set up an immediate backup of any technical equipment in the affected area. In case of data centers, the company will send their data to the data centers which have less then needed data. The bandwidth issues will be discussed by the members of the intrusion detection team and resolved thereof.
2. Similarly, in case of earthquake, complete evacuation of all the buildings will be undertaken and a similar procedure of backup will be adopted if the earthquake is strong only in a locality.
3. For cyber security scenarios, the following scenarios will be seen and understood.
   * + In case of a denial of service (DOS) or DDOS attack, the company will try to use its backup servers in order to mitigate effects of the attack on the server. The part of the server that is recognized in the assessment procedure as the most critically hit, will be shut down and rebooted using the backup machines, if necessary. There are several DOS mitigation and DDOS mitigation software that are developed and deployed by companies for such scenarios. Such software can be used for the complete security of a server from such attacks. The incident response team will be responsible for complete recovery of the servers and the systems.
     + In case of a spoof attack, all outward communication channels will be encrypted, as the person eavesdropping on our communication will have no idea about what is happening and will get his channel flooded with garbage. The members of the incident response team will then be given the task of analysis on the connected IPs to recognize the system from where the cyber-attack is being initiated. The cyber-security wing of the law enforcement agencies will then be contacted for further investigation of the matter, if the actions of the culprit are out of the law.
     + In case of a worm break-in, the malware research department of the incident response team will be given the task of researching on the worm that has broken in to the system. The intrusion detection and prevention systems come in very handy when talking about the pieces of code which attempt to weave its way past the network security architecture. One such example of an attack is the one carried out on the Iranian nuclear facilities.

## Disaster Recovery Procedures

### Emergency response procedures

The appropriate emergency response is required to a fire, natural disaster, or breach in order to protect lives and data and limit damage. The damage caused to assess also include loss of data at computing systems. It can be physical loss of data or at such vulnerable times, the hackers attack to steal data. It greatly effects the data security and business of numerous. For such incidents business emergency response procedures are prepared and implemented. These now also include plan to avoid security breaches during a catastrophe as there is huge need to address the issues of integrity and confidentiality of data.

### Backup operations procedures

It is very important that essential data processing operational tasks can be conducted after the disruption. Backup solution might not be able to stop the loss of data but will provide means to recover the data quickly.

### Recovery actions procedures

The recovery actions aim to facilitate the rapid restoration of a data processing system following a disaster. The data can be transferred to a secure location and be recovered in better conditions. It is arguable that Data security is a significant part of Business Continuity Plans for any organization. It sets parameters of authorized access to systems and information during disaster and recovery period. It also defines the measures which are essential to stop intrusions.

## Incident response team charter

### Executive Summary

From today’s reality and cybersecurity issues, it is evident that every organization needs a constant and vigilant solution against the breaches. Thus, this proves the significance of a vigorous incident response plan and team who executes this plan. IBM has a IBM X-Force® Incident Response and Intelligence Services (IRIS) team in place which helps minimize the damages and offers a detailed overview on the incident so that effective future strategies can be made accordingly.

### Mission statement

The mission of an IRT team is to practice their collective knowledge, skills and experience to ensure a safer and more secure global electronic environment, even in case of a disaster. The team prepares for and respond to any type of emergency that may affect the business.

### Incident Declaration

The incident will be declared by the head of the team. He will be the one responsible for the assessment of the threat and the declaration of the severity of the incident.

### Organizational Structure

There are a number of ways that the organizational structure can be arranged and the one that will work best for this IRT is known as the central organization structure. The decision-making procedures of the company will be kept centralized so that the team moves and works in one direction and as a unit.

### Roles and responsibilities

A team provides an incident response support in several ways. Firstly, an on-site incident response services are offered directly to the constituent. Secondly, the Incident response services are provided virtually through an email or telephonic conversation. In addition to this, coordinated incident response services which merge and assign the efforts of various incident response teams across several constituents.

### Information flow and methods of communication

After an incident hits an organization’s IT substructure, the response team has to address internal as well as external communication requirements additionally to technical matters which include investigation, suppression and recovery. Communication strategy should also include agreement related problems, media communications and also internal communications. There must be suitable balance between directness and defense. If more information than necessary is revealed, it could outcome in excessive increase or revelation of an exploitable problem which was not yet resolved.

### Methods and services provided by the IRT

The IRT can be seen as the emergency force of the company. It provides support and technical help in case of emergencies. The following services and products can be launched by the IRT in order to solve the problems related to incidents.

* First aid training to employees to raise awareness regarding first aid and its deployment.
* Utility based First aid kits.
* Anti-fire blankets and fire extinguishers: Most of the time if a human being catches fire, the most appropriate response is trying to extinguish the fire by any means possible.
* Facility evacuation drills.
* Immediate data backup drills.

### Authority and Operating procedures

In the IRT, there is a head of all departments who is the de-facto leader of the team. He is followed by heads of departments. Every head of department is responsible for performing the restoration action in its own department. They are then followed by the team which report to them.

References:

Lombardo, J. (2017, June 4). IBM’s Mission Statement & Vision Statement (An Analysis). Retrieved December 12, 2019, from Panmore Institute website: http://panmore.com/ibm-vision-statement-mission-statement-analysis-recommendations

MSA. (2019, July 15). IBM Mission Statement 2019 | IBM Mission & Vision Analysis. Retrieved December 12, 2019, from Mission Statement Academy website: https://mission-statement.com/ibm/

Appendix:

