ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (76-78), Month: July - September 2022, Available at: www.researchpublish.com

Are unannounced drills a categorical imperative for Information Technology (IT) Systems?

Asad, Adli M.

Dhahran, The Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7085751

Published Date: 16-September-2022

Abstract: **Enterprises are always challenged by deciding on the cost/benefit of Disaster Recovery (DR) investment. Organizations readiness to respond to threats whether it's natural disasters, cybersecurity, or human induced is vital for its Business Continuity Program (BCP). Therefore, training/drills/exercises provide measurable assurances that critical functions/system are resilient to unplanned incidents. IT professional though have a consensus on exercising announced drills but disagree on the value of unannounced drills.**

This article is an attempt to describe and examine the value of unannounced drills by using the method of doubt approach by the 17th century philosopher named René Descartes to conclude the verdict.

Keywords: **Information Technology, IT Disaster Recovery (DR), Controls, Critical Systems, Business Continuity (BC).**

I. INTRODUCTION

BCP is considered vital to organizations resiliency. The role of IT is to enable the business and address challenges regarding availability. Complex integrations of systems combined with ever-growing cybersecurity threats expands vulnerability of IT systems. Therefore, the existence of a solid DR plan is mandated by most corporates. Important fact readers should keep in mind is the amount of resources organizations have to bear to conduct a yearly calendar DR drills to ensure IT readiness for credible threats and ensure capabilities are in place.

In addition, this document covers a brief on IT DR plans and address organizations requirements for development of IT Disaster Recovery Plan (DRP).

II. IT DISASTER RECOVERY PLAN (DRP) BRIEF

In first stages, let us highlight IT DRP main modules:

1. **Executive Summary**
2. **Scope**

a. In scope

b. Out of scope

3. **DR Policy**

a. Governing documents

b. Data Proponents

c. Data Custodian

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (76-78), Month: July - September 2022, Available at: www.researchpublish.com

4. DR Roles and Responsibilities

a. IT Management

b. DR Incident Commander

c. DR Technical Team Leaders

5. Recovery Plan Activation

a. Activation of the DR Plan

b. Start of Recovery Process/Procedures

6. Return to Normal Operation

a. Deactivation of the DR Plan

b. Recovery of Normal Operation

Next, let us define the scope of IT DR services and using the below classification:

Classification	Description	Backup
Tier 0 Mission-Critical	Infrastructure	
Tier 1 Mission-Critical	System/application	Synchronous or continuous data replication
Tier 2 Important	System/application	Asynchronous continuous data replication
Tier 3 Non-critical	System/application	periodic data replication

The classification process is called Business Impact Analysis (BIA) where Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) are determined. Two main factors are considered during the BIA process; impact of the risk posture from the unavailability of a business function and the likelihood of the risk to be realized.

Last challenge is organizations adherence to constantly ensure an up-to-date disaster recovery plan (DRP) is ready for anytime anywhere disasters.

III. DRP TRAINING/DRILLS/EXERCISES

The awareness program of IT drills is a fundamental practice within the Business Continuity program and establishing a yearly calendar DR drills plan is mandated by most IT and cybersecurity governing documents.

There are multiple types (tabletop and others) of drills, however our focus are:

1) IT Announced DR Drills:

Let us start by examining announced drills claims. First let us try to doubt the objective and validate if it's clear and distinct? Announced drills objective is to tests the execution of DRP which results in the verification of business process, people and technology. The scope of testing is comprehensive and the outcome ensures continues improvement/Remediation of any reported observation. In addition, each drill preformed will typically yield a lesson learned that the DR execution team can share with the training program to enhance future DR executions. I addition, a good IT drill scenario should vary to include three main drills variation:

- Application
- Cybersecurity
- Cloud services

Executing announced drill in the above fashion leaves no room for speculation and ensures all possible readiness are in place. Therefore, I believe announced drills are fit for purpose and all organizations should focus on this type of drills.

2) IT Unannounced DR Drills:

Now let us evaluate the objective of unannounced drill and the claim that it is captures real life lessons. First, let us examine the premise of capturing real life lessons by assuming that its valid and see if this approach can lead us to true value? As with any testing, environment plays a great role in determining the outcome.

For example, preforming an unannounced drill in business day vs a weekend may yield different outcomes. Similarly, the test will vary based on the business activities taking place at the time of the drill. Therefore, capturing all possible combination of variables for a specific environment is not pragmatic.

Next, let examine if unannounced drills can assess staff performance under duress situations. The claim definitely has a merit, however as we have learned from previous experiences that humane behavior is complex and again multiple factors come in to play to conclude an objective lesson.

However, the value of unannounced drill maybe justified under specific premises such as testing Incident Response plan where the stacks are high as it's related to health and safety.

As for IT DR drills, a better alternative is establishing a professionals training program combined with well-defined Polices/Process/Procedures to meet the target objective.

Executing unannounced drills creates a double jeopardy risks each time drills are preformed and the corporate cost outweighs any credible benefits. Therefore, I believe as a business Continuity professional that unannounced drill are represent risks to IT operations and corporates should minimalize this sort of drills for IT systems.

IV. CONCLUSION

Unannounced drills sound like a great idea until you apply the method of doubt to conclude that it does not represent the value you hope for. Therefore, my verdict is for corporates to direct company resources and funds toward the below programs/technologies that focuses on disaster prevention:

- Invest in advanced monitoring tools for critical applications
- Resilient Software development (infrastructure independent) for applications
- Establish/Invest in Enterprise Risk Management (ERM) program
- Establish/Invest in Business Continuity (BC) Program
- Continuous development of DR scenarios/Drills/Training

Figure 1: illustration of programs/technology with proven value.

REFERENCES

[1] Disaster Recovery Institute (DRI) web site https://drii.org/
[2] Gartner web site https://www.gartner.com/en
[3] NIST website https://www.nist.gov/
[4] Professional Business Continuity experience with large enterprise
[5] On-line research from multiple business Continuity articles, however no article found addressing the specific subject.