AMCIS 2015 Puerto Rico Paper Submission

Applying Cyber Range Concepts of Operation to Disaster Recovery Testing. A Case Study

Emergent Research Forum Papers

Victoria Kisekka
State University of New York at Buffalo
vkisekka@buffalo.edu

Corey Baham
Louisiana State University
cbaham6@tigers.lsu.edu

Abstract

A critical component of disaster recovery planning is testing, which involves verification of the effectiveness of the DR solutions. Currently, there are several limitations that plague disaster testing efforts such as the inability to create realistic disaster scenarios and test them in a production environment. Cyber Range Concept of Operations (CONOPS) presents an opportunity for overcoming these challenges. The purpose of this study is to demonstrate the application of Cyber Range CONOPS to DR testing. We use a case study approach to observe the development of a disaster recovery program in a large enterprise. We seek to gain an insight into the design and implementation of a disaster recovery program, using the concept of Cyber Range.

Keywords

Disaster recovery, disaster recovery planning, cyber range concept of operations, cyber ranges.

Introduction

Disruptions caused by natural and man-made disasters pose significant challenges and risks to an organization’s operations. There are some actions that can be taken before a disaster occurs to mitigate the impacts. One such action is Disaster Recovery (DR) planning which, unfortunately, is widely misunderstood (Smith & Wenger, 2007). A critical component of DR is testing, which involves verification of the effectiveness of the DR solutions. Testing an organization’s DR solutions aims to identify inefficiencies in the DR programs. For instance, testing outcomes may include identification of the necessary DR resources, how long it would take the organization to recover following a disaster, etc. Without testing, there is no guarantee that the DR solutions will work. Also, there are different types of disasters, each of which vary in impact and as such bring different challenges. A significant limitation that plagues DR testing efforts is the inability to create realistic disaster scenarios and test them in a production environment. There is also a lack of data to effectively assess DR plans (Altay & Green, 2006). Cyber Range Concept of Operations (CONOPS) presents an opportunity for overcoming these challenges. Cyber Range CONOPS were developed by the Defense Advanced Research Projects Agency and involve the use of realistic assessments of the effectiveness of cybersecurity tools (Pridmore, Lardieri, & Hollister, 2010). The process employed in Cyber Range testing typically involves modeling cyber attack scenarios and applying real-world cybersecurity tools to resolve them. Evidence suggests that Cyber Range CONOPS have several benefits including scalability, cost efficiency, and identification of security vulnerabilities (C. Siaterlis, Garcia, & Genge, 2013).

When applied to DR, Cyber Range CONOPS techniques offer opportunities for testing the effectiveness of DR plans by realistically emulating disaster scenarios in a controlled environment with the objective of
evaluating risks, business impact, and relevance of the plans. With this approach, insights gained during the DR testing may be used to improve upon the DR programs, consequently strengthening the organization’s ability to mitigate the impact of a disaster. A significant benefit of leveraging the concepts of Cyber Ranges lies in their flexibility; specifically, they are scalable, easily reconfigured, and can be repurposed as needed (Pridmore et al., 2010). These benefits would also be realized in DR testing, allowing for an evaluation of different business scenarios and disasters.

The purpose of this study is to demonstrate the application of Cyber Range CONOPS to DR testing and preparedness in general. We use a case study approach to accomplish this objective. In particular, we observe the development of a Disaster Recovery Program (DRP) in a large enterprise. The DRP comprises of DR training and DR testing. We seek to gain an insight into the design and implementation of a DRP. The rest of the paper is organized as follows: The following section discusses the literature in DR testing and Cyber Range CONOPS. Next, we present the theoretical underpinnings of this research. Lastly, the methodology and future work are discussed.

Literature Review

Disaster recovery testing

The viability of a DR program is examined through a process of testing to verify that the plan will work when executed during a real disaster. There have been several studies discussing approaches to DR testing. The approaches discussed in the literature mainly focus on modeling disaster response scenarios (Beamon & Kotleba, 2006; Bryson, Millar, Joseph, & Mobolurin, 2002; Najafi, Eshghi, & de Leeuw, 2014; Pidd, de Silva, & Eglese, 1996). Other researchers have focused on data recovery. An example of such studies include Holdman, Kavuri, Rassbach, Hammett, and Ward (2007)’s work where the a data DR system was developed. The proposed system provided redundancy using virtual snapshots of data libraries. The DR testing technique applied by the authors involved the use of extra virtual libraries (Holdman et al., 2007). Closely related are studies whose focus has been on designing algorithms that support DR testing. Some examples include Haghani (1997)’s optimization models for disaster management, a model for managing vehicle routing during disaster response (Zidi, Mguis, Borne, & Ghedira, 2013), and a resource management model by Najafi, Eshghi, and Dullaert (2013).

In the area of Information Systems, the process of fault-tolerant testing is often performed. This process is similar to DR testing and involves the assessment of fault tolerant systems, which are designed to provide backup functionality in the event that the main computer systems fail. A procedure called fault injecting is widely used for testing and is performed by introducing faults in the backup systems and evaluating their performance (Avresky, Arlat, Laprie, & Crouzet, 1996). Different types of faults can be injected to allow testing of various scenarios. Evidence suggests that this approach to testing can be applied to software programs, hardware systems, servers, operating systems, virtual machines, and computer networks (Buchacker & Sieh, 2001). While the techniques used for injecting fault injections vary, the objective is to evaluate the effectiveness of the DR or fault system.

Cyber Range Concept of Operations

As described earlier, Cyber Range CONOPS facilitate the evaluation of an organization’s security posture. Cyber Range CONOPS assessments offer opportunities for realistic and more accurate evaluation of cybersecurity solutions. However, as of the writing of this paper, their application and research is still in its infancy.

The current literature on this topic broadly falls into two categories. First, is the literature proposing design solutions for developing Cyber Ranges, with a focus on resource management, adaptability to various scenarios (Rosenstein & Corvese, 2012), scalability through modular design (Lawless, Flood, & Keane, 2014), and their applicability and efficiency (Genge, Siatelis, Nai Fovino, & Masera, 2012; C. Siaterlis et al., 2013; Varshney, Pickett, & Bagrodia, 2011). Elsewhere, researchers have proposed Cyber Range designs called ‘clusters’ and ‘overlays’ (Christos Siaterlis & Masera, 2010). The term cluster describes a Cyber Range where the testing environment is separate from the production environment, while in overlay, the testing is completed in the production environment (Christos Siaterlis & Masera, 2010). The second research category is the application of Cyber Range concepts. Current application
areas of Cyber Range CONOPS include software, hardware, and computer networks (Genge et al., 2012; Christos Siaterlis & Masera, 2010; Varshney et al., 2011).

Cyber range concepts have not been applied to the DR area, yet they present an opportunity for overcoming the current limitations in DR testing by providing a realistic approach to evaluating the vulnerabilities in DR programs. Our method of DR testing facilitates the emulation of different types of disaster scenarios, all within a controlled environment. In the next section, we discuss the theoretical foundation of this work.

**Theoretical Background**

*Technology-Organization-Environment Framework*

The theoretical underpinning we use in this study is the Technology Organization Environment (TOE) framework (Tornatzky, Fleischer, & Chakrabarti, 1990). According to the TOE framework, there are technological, organizational, and environmental processes which impact the adoption of innovations (Tornatzky et al., 1990). The technology context takes into account all the organization’s technologies, including existing technologies already in place, and new technologies that might be required. The organizational context deals with organizational-level attributes; these are the characteristics of the firm that may influence the adoption of new technologies. Lastly, the environmental context is concerned with social processes within the organization.

This research uses the TOE framework to guide development of a Cyber Range CONOPS for DR testing. Within the technological context, we focus on the technical resources employed to build the DR testing environment. For the organizational context, we focus on identifying the organizational resources needed for developing the DR tests. Here, the emphasis is on technical resources such as the knowledge and skills of the technical team, which are considered to have a significant influence on technology innovations (Kuan & Chau, 2001). In regards to the organizational context, we consider the internal influences within the organization. Organizations face different disasters, which are characterized by uncertainty and may require different techniques to mitigate their effects. Therefore, improving the organization’s ability to respond requires understanding the influence that each type of disaster exerts on the organization’s services and how to better manage them. The aspects of an organization’s internal environment that we focus on are the different disaster scenarios.

**Case Study**

*Methods*

To gain an insight into the design and implementation of a DRP using Cyber Range CONOPS, we use a case study methodology. This empirical investigation will be conducted in an on-the-ground exploratory study of a large healthcare enterprise, which will be referred to as Arrow Star. Our case study approach is suitable for investigating phenomenon in its real life context (Yin, 2013). Also, the approach we employ is guided by the recommended process for conducting case studies (Klein & Myers, 1999).

*Research site*

In this research, we focus on the complexities associated with DRP. Such complexities are driven by a large number of interacting and interdependent components from different parts of the organization, at a time when teams need to work in unison to recover systems. These types of complexities are generally experienced by medium to large sized organizations that strive to implement active-active redundant datacenter environments, with production networks that stretch across primary and secondary sites. These types of organizations struggle with the isolation of production systems as they attempt to conduct comprehensive disaster recovery tests. Also, the risk of contamination of production systems due to disaster recovery testing activities may potentially grow due to human error while conducting complex activities such as isolation of the primary datacenter to conduct tests.
The organization used in this case study, Arrow Star, offers healthcare services in the U.S.A. and has a robust Information Technology (IT) staff that manages over 1,500 servers; maintains, designs, develops, and supports over 250 applications. Arrow Star’s disaster recovery department has difficulty testing its production systems in a secure and realistic setting because of its current connectivity and dependencies across systems. To overcome these difficulties, a DRP will be developed based on the concept of Cyber Ranges.

**Data collection and analysis**

This research uses direct observation, informal interviewing, and collecting artifacts as the primary tools for data collection. This process started in January 2015. One of the authors, who was formerly employed at Arrow Star, visited the company two times a week to attend office meetings, discuss the progress of the DRP, and collect artifacts pertaining to the DRP design. Thus far, direct observation of the DR Manager and IT team interactions have formed the majority of the field research. Notes were taken during the interactions.

**Preliminary findings**

Because this is a study in progress, we report our initial findings from the interviews and observations that have been conducted thus far. These initial findings relate to the key factors in Arrow Star’s DRP design requirements as the company prepared for its DR testing. The critical requirements were:

1. Flexibility. The DRP must allow for continuous access to realistic, hands-on DR training and testing. This allows for the continuous testing of DR capabilities as needed.

2. Isolation. The DRB must ensure isolation of the production environment to avoid any type of contamination from DRB activities; these types of tests can be disruptive to production and could compromise system stability and corrupt data.

3. Comprehensive. The DRB must allow for testing of current production systems and their interactions so that technical staff can acquire greater technical expertise in the recovery of these systems.

4. Readiness. The DRB must provide the capability to assess its people, processes, and technology readiness within a “real-world” environment.

5. “Real-World” The DRB must incorporate the structural and people complexities representative of the real world—allowing for the realistic testing of all the components of DR, including dependencies to people, processes, and technologies.

**Future work**

Next steps include observation of the actual development of the DRP and interviewing the IT team throughout the process and analyzing the data.

**REFERENCES**


