International Journal of Information Management 37 (2017) 622–626

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Research Note

Disaster recovery plan for medical records company

Vincent Lozupone

Northcentral University, 2488 Historic Decatur Rd. San Diego CA 92106

ARTICLE INFO

Keywords:
Restore
Windows
Server
Disaster recovery
Intrusion detection
Threats
Virus

ABSTRACT

Computer systems have become a critical part of many businesses. Businesses rely on computer systems to perform many daily tasks. It is important that businesses have a valid strategy to recover their data in the event of fires, hurricanes, other natural disasters, sabotage, or security incidents. This paper describes the concepts of a disaster recovery and data replication plan that The Medical Record Company will adhere.

1. Introduction

The Medical Records Company depicted in this report can be any company, regardless of size, which deploys Windows servers that may choose to use this document as a guide for planning for a disaster recovery. Medical Records Companies are firms that offer Information Technology to hospitals, medical labs and other various healthcare organizations. It is important to note that even though a company of any size can use this strategy, a large company may use more resources that are needed to assure a plan that is sound and feasible. Although this report focuses on Microsoft products, facets can be applied generically, i.e. RAID, vulnerabilities, offsite storage, disaster recovery plan, and steering committee.

The Medical Record Company's (MRC) network is configured as a single Microsoft Active Directory Domain. Each client company is using Windows Professional as the operating system. There are four sites connected by broadband, and each site is managed by a LAN administrator. The company is also using WINS, DNS and DHCP at each site. The DNS configuration is using dynamic updates. There are also 20 file servers running the Server 2012R2. This report will identify vulnerabilities with a mitigation strategy, disaster recovery plan and finally present an effective intrusion detection design.

2. Identify the vulnerabilities in the current configuration and describe how to mitigate them

A hardware failure can also be considered an exposure and MRC considers this type of failure a natural disaster. Manmade disasters can be sabotage, arson, strikes, bombings, and unavailability of key employees. MRC will obtain relevant information from insurance companies, local weather service, law enforcement, and newspapers. This information should include statistical data from weather and site studies from the Government of an impact study. This should also include man-made risks (Sans Institute, 2002). Irrespective of the type of disaster, aside from a security incident, the disaster recovery will have the same plan.

The 20 file servers will be backed up to tape backup system using an incremental configuration. See Fig. 1 for types of backups. An incremental backup only requires the last full backup and the last incremental backup to acquire a full recovery. The tapes will be stored off site at a company, for example, IronMountain.com or similar. This plan will also entail purchasing a server with a backup tape and software and assuring that there is a location to perform a restore if necessary. MRC will be purchasing Paragon Hard Disk Manager Suite 2011 (see Fig. 2). MRC will also have fault tolerant storage. RAID (Redundant Array of Independent Disks) configurations will be configured on all servers. The system drives will have RAID 1, disk mirroring. This will yield redundancy and excellent read and write performance. During a failure the alternate drive will take over (Cole, 2008). The remaining drives will have RAID 5, striping with parity. The workstations will be managed with Symantec Ghost Solution Suite 3.0. This software will deploy new workstations and restore in case of a disaster. MRC will use Symantec's Data Loss Prevention as part of the suite.

According to Developer Network (2015), most people think that defining security vulnerability would be easy. It is not. Security vulnerability can be a potential attack on a system, for example malware, incorrectly configured systems or passwords scribed on a pad. Vulnerabilities can be security exposures that may result from a product weakness by a business producer introduced by accident or an intended attack. MRC considers the lack of a plan, business impact assessment,

E-mail address: vlozupone@hotmail.com.

http://dx.doi.org/10.1016/j.ijinfomgt.2017.05.015
Received 5 May 2017; Received in revised form 11 May 2017; Accepted 26 May 2017

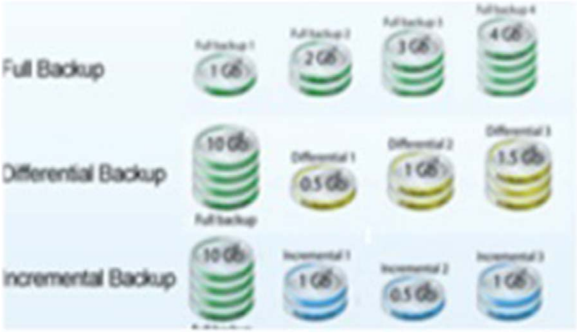

Fig. 1. Backup Types (Images, 2017).

Fast & Easy Recovery

- **Complete Restore** - restore your computer to an earlier state without losing data, reinstalling and reconfiguring your programs.
- **Recovery based on need** - an entire disk, separate partitions or specific files.
- **Create bootable rescue media** with NEW Recovery Media Builder 3.0

Fig. 2. Paragon (Paragon, 2015).

business continuity plan, a security assessment and a detailed definition of requirements a vulnerability. It is imperative that MRC, from an economic and business strategy perspective focus on the activities that have the effect of reducing the likelihood of a disaster occurring rather than focusing on minimizing the impact of the disaster (DRP, 2013).

Since there are four sites, there has to be a dedicated communications between all the sites. There also has to be replication existing for WINS, DNS, and DHCP. When configuring WINS replication, there are two issues that need to be considered, type of network and the length of time required for all replicated changes in the WINS database to converge (Technet, 2005). The Converge time is the time needed to replicate a new entry in a WINS database server. MRC will test the network throughput to determine this parameter. Dynamic DNS enables client computers to register and dynamically update their resource records with a DNS server upon changes. This alleviates the need for manual intervention. DNS will be configured on all the domain controllers. Server 2012R2 has a new feature that enables Microsoft DHCP servers to share service availability information providing DHCP with high availability. It works by replicating IP address leases and settings in one or more DHCP scopes from a primary to the failover server. All zone data will be replicated to all other domain controllers to each site (Fig. 3).

Another vulnerability that MRC has to respond is a security incident. MRC will create a plan that deals entirely with recovering from a security incident (Cole, 2008). This plan will use the industry standard name of Computer Security Incident Response Plan (CSIRP). This plan will provide MRC with the precise information needed at the critical moment that an attack is recognized or suspected. The first step that MRC will do is to build a team called Computer Security Incident Response Team (CSIRT). Each member of the team will have a definite role to play. Each site administrator will be aware of the network topology, configuration of the servers and desktops and be aware of the applications installed on the workstations.

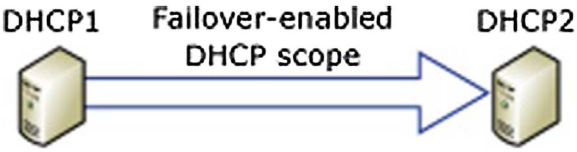

Fig. 3. DHCP Failover (Lozupone, 2015).

Table 1
Severity Classifications.

Severity	Type
1	A few users have received an email with a virus attachment
2	Scans have detected possible targets
3	Many scans detected on perimeter. Many computers affected
4	A breach has occurred or a DOS (Denial of Service) was successful.
5	A major impact on production has occurred. Financial or medical information at risk.

MRC will determine the severity level assigned to each type of incident. MRC has created a table that will assign a severity to a designated type. Severity 5 is the most serious and has the potential of financial loss to the company as a result of the possibility of health records being comprised. This can also have a damaging effect on the image of MRC and must be taken very seriously. See Table 1 for severity classifications.

3. Design and develop intrusion detection and prevention controls for this organization

There are a few techniques and groups that make up intrusion detection systems. Also, there are signature-based and statistically anomaly-based systems. There are advantages and disadvantages to both. Effective IDS (Intrusion Detection System) systems can use both. A signature-based ID stores signatures of attacks as a reference. When data is collected in a log and if there is a match a response is initiated. One weakness of a signature-based ID is a failure to catch attacks over a long period. Other weaknesses include resource intensive to the system, and they are OS (Operating System), platform, and application dependent.

Statistical anomaly-based IDs compare learned and normal behavior patterns and will trigger alarms when an anomaly occurs. To work correctly, the ID has to take a sample of network patterns over a long period. These patterns are memory usage, CPU utilization, and network packets. Some advantages are, it is dynamic, OS agnostic and can prevent abuse-of-privileges attacks. MRC will use both types.

MRC will also implement a NIDS (Network–based). See Fig 4 for a comparison of NIDS vs. HIDS and Fig 5 for a depiction of NIDS flow. It resides on the network and monitors the entire network, and since MRC does not have network segments, it is a good solution. It works as an appliance in conjunction with a NIC (Network Interface Card). The NIC is configured in the promiscuous mode. This mode sees *all* traffic on the network. As packets pass through the network, the NIDS inspects and identifies packets that are suspect. It looks for a string, port and header condition signatures. An NIDS customarily provides reliability with the absence of consuming network or host resources. It also provides real-time information (Cole, 2008). Stallings (2007) stated that sensors can be either passive or inline. Most NIDS are deployed using the passive mode. A passive mode monitors a copy of the traffic and actually does not pass through the device. Therefore, no packet delay is realized. MRC will use the passive mode (Fig. 6).

An IPS (Intrusion Prevention System) is very similar to the IDS. The difference is that the IPS will attempt to prevent attacks instead of only logging. MRC will install IPSSB (Intrusion Prevention System Software Blade) from Checkpoint at each site (Checkpoint, 2015). It has