U13A1

You are a security analyst for Ohio University in Athens Ohio. You have been approached by the CIO and the director of infrastructure about a report released by the CDC. They have asked you to fill in the attached DR plan based on this report released by the CDC:

<https://stacks.cdc.gov/view/cdc/6023>

Have fun with the information and don’t fret about specifics. You will be making-up some of the information as you go along. This assignment is a balance of fun and hypothetical.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Not Met | Basic | Proficient | Distinguished |
| Completed relevant information (20 points) | Did not complete information needed (0) | Completed most of the information with no errors (1-10) | Completed all information with no errors (11-19) | Went above and beyond minimal requirements (20) |
| Demonstrates knowledge of DR (15 points) | Did not demonstrate knowledge (0) | Demonstrated basic level knowledge of DR procedures (1-7) | Showed a proficient grasp of DR policies and procedures (8-14) | Showed an advanced level of DR policies and procedures (15) |
| Grammar and structure (15 points) | Student submission is below college level writing expectations (0-5) | Multiple grammar and structure issues (6-11) | Little to no grammar and structure issues (12-15) |  |

Course Outcomes Assessed:

5. Identify and evaluate threats, vulnerabilities, countermeasures, and mitigation recommendations.

8. Create a business continuity and disaster recovery plan.

## DISASTER RECOVERY PLAN

## USE IN CASE OF ZOMBIE ATTACK

##### VOIP/Email Recovery

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Application Description** | | | | | | |
| Recovery Priority: | Critical - Communication | | | | | |
| Application Name: | VOIP / Email | | | | | |
| Application Description: | VOIP phones on campus of Ohio University and Email system | | | | | |
| Software Modules/Current Version: | Up-to-date Cisco Unity system / Exchange hosted in Office 365 Cloud | | | | | |
| Vendor Name: | Cisco / Microsoft | | | | | |
| User Location & Departments: | Athens, Ohio – Office of Information Technology (both hosted by infrastructure team. | | | | | |
| **Technical Support Information** | | | | | | |
| Vendor Support phone #’s & Web Site | 555-555-5555 | | | | | |
| Vendor Account and/or Technical Contact Name & Number: | 10-987234 | | | | | |
| Server(s) name:  Server type:  Server OS:  Server Location:  IP Address: | Cisco Unity network / Cloud based email hosting | | | | | |
| Vendor access method: | Remote Desktop | | | | | |
| Modem Numbers: | None | | | | | |
| **System Notes** | | | | | | |
| Interface Engine: | NA | | | | | |
| Interfaces – Inbound: | NA | | | | | |
| Interfaces – Outbound: | NA | | | | | |
| Other Comments: | NA | | | | | |
| Maintenance and Recovery Procedures | | | | | | |
| Maintenance | Check for patches every other week.  Install updates every month as needed. | | | | | |
| Backup Method/Schedule | Backup data to the cloud every two weeks.  Backup data to a physical storage every week. | | | | | |
| Support Personnel | | | | | | |
| Name | Site | System | Office | Pager | Home | Cell |
| Systems Administrator: | J Smith |  | 555-5555 |  |  | 555-3454 |
| Other Administrator: (PHNS or Customer) |  |  |  |  |  |  |
| **Last Updated:** | 7-1-2014 | | | | | |

# Recovery Procedures

This section describes the recovery strategies identified for the equipment and services. Include notation for the following: **Criticality Priority**; Other System Dependencies; SLA System (Y/N); Estimated Time to Restoration.

**Assumptions**

These recovery procedures rely on the following critical assumptions. If any of these assumptions are not true at the time of the disaster then the user facility must remain in downtime procedure mode until all such assumptions are true.

* VOIP / Email communications is mission 24/7 mission critical – During a zombie outbreak, having a form of communication will help with ensuring safety across the campus and keep updates on the situation.
* Specific Key Staff needs to stay on-site – Leaving the site would be dangerous as the journey home and back has the potential to attract the attention of the zombies and could lead to the key staff being turned or unable to get back to the work when needed.
* These need power and internet or local network for operations – The communication is sent through phones and computers making the need for internet and the local network important and the power to be able to send and receive the messages. Messages can not be spread through out campus on speakers as it could attract the zombies.

**System Architecture**

**Software & Hardware:**

Cisco Unity Gateway is locally hosted on a server rack in the Computer Services building.

**Back-Up Schedules:**

Insert information concerning backup strategy: Such as backed up by PHNS Operations & Systems staff according to the following schedule. All tapes are stored in a secure vault off site, etc.

| **System Component** | **Server** | **Frequency** | **Method** | **Comment** |
| --- | --- | --- | --- | --- |
| Cisco Unity Gateway | Hewey | Daily | Network | Check frequently |
| Network Switches | Lewey | Weekly | Network | Check for any disconnects |
| Router | Dewey | Weekly | Local | Check router box |
| Local Exchange Router | Chewey | Daily | Local | Locally and needed |
| Barracuda SPAM device | Phewey | Weekly | Local | Keeps spam out |
|  |  |  |  |  |
|  |  |  |  |  |

**Procedures**

# Server Recovery Procedures: (include server restoration priorities)

# Hewey

1. Follow steps located on the Cisco site.

# Lewey

1. Check the connection and configuration, use any back up as needed.

# Dewey

1. Turn it off and on again. Check the wiring and the connection.

# Chewey

1. Turn it off and on again. Check the wiring and the connection.

# Phewey

1. Check the physical appliance and the wiring. Turn on and off again. Check the connection.

# Staff Needed to Protect Servers (contact tree)

1. Sandra Davis 555-443-2187
2. Andrew Warren 990-678-3241
3. Chris Redfield 555-978-2234

# Physical/Cyber Security Concerns: (If warranted)

1. Zombies enter the inside area.
2. Can not get spare parts in case of something breaking.
3. Must be able to keep power going.

# List supplies needed to protect servers and support staff

1. Food, water, and blankets.
2. Weapons for attacking the zombies.
3. Fencing or a physical perimeter.
4. Spare parts.
5. Generator

# Other Considerations

1. Consider the amount of activity outside.
2. Too many gathering zombies can lead to a break in.
3. Workers who go outside need to be checked for any afflictions from zombies.
4. Determine whether to take in survivors and train them in case a worker falls.