**Disaster Recovery Policy Creation Guide**

**Goal**: A disaster recovery policy related to information security for a company should cover three topics:

1. What measures are being taken to mitigate or prevent data loss?
2. What measures are being taken to prevent hacking or security compromise?
3. What procedures can be used to recover data in case of a security breach.

A good recovery policy will briefly address the 1st and 2nd points, and describe point 3 in detail for all systems and portions of critical data.

**Requirements:** This inject involves collecting some information about what you and your teammates have done to backup your systems, and then a lot of writing to summarize the information and create a policy. Leave yourself plenty of time for the writing, it's probably more important than the technical aspects. Any time you mention a specific technical implementation, make sure you have prove of its existence and functionality.

**Steps:**

1. Take a survey of all critical data and whether or not it is being backed up. If it is not, start doing that ASAP. If convenient, this may be a time to move towards a more unified and comprehensive solution for backups.
2. Write a detailed summary of the backup processes and plans for this data. You may want to organize this information by individual machine.
3. For each piece of critical data you discussed above, describe the process that would be necessary to restore in from your backups if it were lost. Note any drawbacks of this process (such as stale data), and approximately how long the process should take.
4. Write a couple of paragraphs about what recent work you and your teammates have done to improve system security. Use a couple of specific examples, but don’t waste excessive time or pixels on this.
5. Compile your work into a policy document. The start of the document should contain an executive summary of your work and the security briefing your wrote in step 4. Then, write the summary of backup implementations and recovery procedures. You can follow the example policy in the appendix of this guide.

**Appendix**

The following is an example response from the 2017 NECCDC qualifier. The response isn’t super complete, and could probably be expanded.

**To:** CIO

**From:** Team 7

**Subject:** Disaster Recovery Plan

**Total Response time:** 120 minutes

**Systems Concerned:** All

**Text Response:**

We have created, and are continuing to refine, an initial disaster recovery plan for our network infrastructure. Below we explain, by host, the actions we have taken to ensure quality of service and recovery following a possible disaster.

**System Name: E-Commerce | 172.20.240.11**

**Platform: CentOs 6**

**Actions taken:** Multiple steps have been taken to ensure a proper recovery Most importantly, multiple back ups have been taken. All files in the web directory have been backed up, also important services such as hppd have been backed up. Furthermore critical files such as etc/shadow/ and /sudoers/ have been backed up. In the event of a disaster, these back ups would be used to reimplement service as fast as possible.

**Actions planned:**

**System Name: UbuntuDNS | 172.20.240.23**

**Platform: Ubuntu 8.04**

**Actions taken:** A thorough review of users unveiled an extraneous “adam” account, this was subsequently removed. Passwords have been cycled to ensure only proper access is granted. Settings have been updated as to prevent DNS recursion from untrusted users outside of the local network.

**Actions planned:** Backups will be implemented in the near future to ensure DNS can be fully restored in the case of an emergency. Updates will also be implemented in key areas to improve the security of this host.

**System Name: Debian Email | 172.20.241.39**

**Platform: Debian Lenny**

**Actions taken:** Multiple backups of configuration files of Dovecot, Samba, and all other email-related software have been taken, so that the system can be easily restored after any malicious attack. Additionally, backups of all email records(as of today) were created to prevent data loss. The server has been hardened through secure passwords for administrative users, no root privileges for non-administrative users, and a firewall to prevent intrusion.

**Actions planned:** In the event of a security breach, system logs will be analyzed to determine what the intruders accessed. From there, any lost data will be restored from the most recent backups, root passwords will be changed, and all email users will be required to change their password.

**System Name: 2003 Server FTP | 172.20.241.9**

**Platform: Windows Server 2003 FTP  
Actions taken:** This host has been powered off in our effort to only run essential services. Team 7 migrated essential services and data to non-obsolete hosts to be able to power off this host..

**Actions planned:** Moving forward Team 7 will properly decommission this host and run a more secure alternative.

**System Name: 2012 Web Apps | 172.20.241.3**

**Platform: Windows Server 2012**

**Actions taken:** On this host administrative passwords were cycled through and an audit of the users and the permissions was explored. A review of the firewall was also undertaken as policies were updated and reviewed to ensure for more secure settings.

**Actions planned:** Moving forward Team 7 hopes to implement proper backups of critical components to ensure a full recovery in the event of a future incident. Security Updates will also be installed once the opportunity presents itself as to be as up to date as possible.

**System Name: 2008 R2 AD/DNS | 172.20.241.27**

**Platform: 2008 R2**

**Actions planned:** To backup the Windows Server, we plan to use the Windows Server Backup Tool and because we don’t have physical access to external drives, we will send the backup files to a shared folder. This will store the backup on another computer, thus allowing us to recover the 2008 R2 server in the case of complete disaster.

To prevent our systems from being accessed maliciously in the future, we have initiated a hardening procedure. This includes disabling remote desktop, disabling the teredo interface, installing important security updates, stopping unnecessary services, reviewing users and disabling potentially malicious users, and analyzing the connections to the 2008 R2 server and terminating unauthorized connections.

To recover data, we plan to schedule periodic system state backups to backup critical files that contain data.

**Actions taken:** The Windows Server Backup feature has been added, and int he future regularly scheduled updated to a secure location will be automated. Furthermore security updates are being implemented to ensure this host is up to date. Extraneous components, like the Teredo interface, have been disabled. Firewall rules and policies have been updated, unneeded services like Remote Desktop Protocol have been blocked.

**System Name: Palo Alto | 172.20.241.100**

**Platform: PAN-OS 6.0.7**

**Actions taken:** Administrative passwords were cycled through and running configurations have been backed up.

**Actions planned:** In the future, more rules will be created, and unwanted traffic will be further restricted.